Windows 8 Tablets

Windows IT Pro

A PENTON PUBLICATION

MARCH 2013 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU



Deploy Windows Server 2012 Roles

Office 365: Top 10 Pros and Cons

A New Approach to Identity Management

Compare File Version Numbers in VBScript and PowerShell

Master Hyper-V Security

1&1 DYNAMIC CLOUD SERVER



SAVE $120 First year*

1&1 DYNAMIC CLOUD SERVER

A fully flexible server for a range of requirements including applications, databases, gaming and much more!

- Independently configure CPU, RAM, and storage
- Accurate and fair: Control costs with pay-per-configuration and hourly billing
- Up to 6 Cores, 24 GB RAM, 800 GB storage
- 2000 GB of traffic included free
- Parallels® Plesk Panel 11 for unlimited domains; reseller ready
- Up to 99 virtual machines with different configurations under one account
- No setup fee
- 24/7 phone and e-mail support

$39.99 per month* ~~$49.99~~ per month*

MAXIMUM FLEXIBILITY
Change hardware configurations in real time to meet your business needs

HOURLY BILLING
Control Costs by only paying for what you configure

MAXIMUM SECURITY
Redundant storage and mirrored processing units reliably protect your server

PARALLELS PLESK® PANEL 11
for unlimited domains

Parallels Plesk Panel

OPTERON PROCESSOR AMD

SUSE

INCLUDES 1 DEDICATED SSL CERTIFICATE

MOBILE APPS
for server management and monitoring



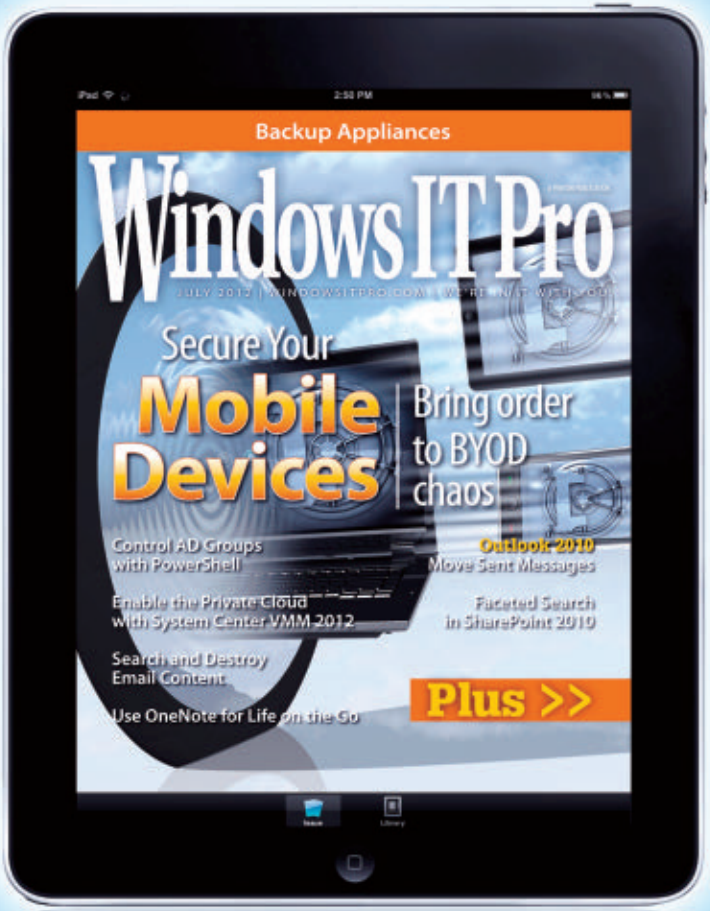
1&1®

MEMBER OF united internet

1and1.com

*Offer valid for a limited time only. Base configuration includes 1 processor core, 1 GB RAM, 100 GB storage. This offer applies to new contracts only. 12 month minimum contract term. Other terms and conditions may apply. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet, all other trademarks are the property of their respective owners. © 2013 1&1 Internet. All rights reserved.

Mobile App
Now Available!



Download your FREE mobile app.

iTunes | Android | Kindle

MARCH 2013 / VOL. 19 / NO. 3

COVER STORY

Windows Server 2012 Deployment — Orin Thomas

39

Learn the necessary steps to deploy Windows Server 2012 as an Active Directory domain controller, as a file server, and as the host operating system for SQL Server 2012, Exchange Server 2013, and SharePoint 2013.



Features

60 Windows Server 2012 Hyper-V Security Features
Jan De Clercq

74 Office 365: Time to Make the Switch?
Tony Redmond

85 Comparing File Version Numbers in VBScript and PowerShell
Bill Stewart

Special Features

58 Windows Server 2012

72 Windows 8

Interact

35 Ask the Experts

In Every Issue

117 Ctrl+Alt+Del

119 Advertiser Directory

119 Directory of Services

119 Vendor Directory

Chat with Us

Facebook Twitter LinkedIn

Access articles online at www.windowsitpro.com. Enter the InstantDoc ID (located at the end of each article) in the Search box on the home page.

Columns

6 IT Pro Perspectives
Windows 8 Myths
Michael Otey



9 Need to Know
Office 2013 and Office 365
Paul Thurrott



15 Windows Power Tools
Meet Set-ADUser, an All-Purpose Hammer
Mark Minasi



19 Top 10
New Features in Office 2013
Michael Otey



24 Enterprise Identity
A New Approach to Identity Management
Sean Deuby



29 What Would Microsoft Support Do?
How Windows Server 2012 Eases the Pain of Kerberos Constrained Delegation, Part 1
Mike Stephens



Products

93 **New & Improved**

97 **Goverlan Remote Control**
Eric B. Rux

101 **CloudPassage Halo**
Russell Smith

106 **Windows 8 Tablets**
Paul Thurrott

113 **Industry Bytes**

Editorial
Editorial Director: Megan Keller
Editor-in-Chief: Amy Eisenberg
Senior Technical Director: Michael Otey
Technical Director: Sean Deuby
Senior Technical Analyst: Paul Thurrott
Custom Group Editorial Director: Dave Bernard
Exchange & Outlook: Brian Winstead
Systems Management, Networking, Hardware: Jason Bovberg
Scripting: Blair Greenwood
SharePoint, Active Directory, Security, Virtualization: Caroline Marwitz
SQL Server, Developer Content: Megan Keller
Managing Editor: Lavon Peters
Editorial SEO Specialist: Jayleen Heft

Senior Contributing Editors
David Chernicoff, Mark Minasi, Tony Redmond, Paul Robichaux, Mark Russinovich, John Savill

Contributing Editors
Alex K. Angelopoulos, Michael Dragone, Jeff Fellinge, Brett Hill, Dan Holme, Darren Mar-Elia, Eric B. Rux, William Sheldon, Curt Spanburgh, Bill Stewart, Orin Thomas, Douglas Toombs, Ethan Wilansky

Art & Production
Senior Graphic Designer: Matt Wiebe
Director of Production: Dylan Goodwin
Group Production Manager: Julie Jantzer-Ward
Project Manager: Adriane Wineinger
Graphic Specialist: Karly Prickett

Advertising Sales
Publisher: Peg Miller
Key Account Director: Chrissy Ferraro • 970-203-2883
Account Executives: Barbara Ritter • 858-367-8058
Cass Schulz • 858-357-7649

Client Services
Senior Client Services Manager: Michelle Andrews • 970-613-4964
Ad Production Coordinator: Kara Walby

Marketing & Circulation
Customer Service
Senior Director, Marketing Analytics: Tricia Syed
Online Sales Development Director: Amanda Phillips • 970-203-2806

Technology Division & Penton Marketing Services
Senior Vice President: Sanjay Mutha

Corporate
Chief Executive Officer: David Kieselstein
Chief Financial Officer/Executive Vice President: Nicola Allais



List Rentals
MeritDirect
333 Westchester Avenue,
White Plains, NY 10604

Reprints
Reprint Sales:
Wright's Media • 877-652-5295

Windows IT Pro, March 2013, Issue No. 223, ISSN 1552-3136. *Windows IT Pro* is published monthly by Penton Media, Inc. Copyright ©2013 Penton Media, Inc. All rights reserved. No part of this publication may be reproduced or distributed in any way without the written consent of Penton Media, Inc.

Windows IT Pro, 748 Whalers Way, Fort Collins, CO 80525, 800-621-1544 or 970-663-4700. Customer Service: 800-793-5697.

We welcome your comments and suggestions about the content of *Windows IT Pro*. We reserve the right to edit all submissions. Letters should include your name and address. Please direct all letters to letters@windowsitpro.com. IT pros interested in writing for *Windows IT Pro* can submit articles to articles@windowsitpro.com.

Program Code: Unless otherwise noted, all programming code in this issue is ©2013, Penton Media, Inc., all rights reserved. These programs may not be reproduced or distributed in any form without permission in writing from the publisher. It is the reader's responsibility to ensure procedures and techniques used from this publication are accurate and appropriate for the user's installation. No warranty is implied or expressed.

Windows®, Windows Vista®, and Windows Server® are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries and are used by Penton Media, Inc., under license from owner. *Windows IT Pro* is an independent publication not affiliated with Microsoft Corporation. Microsoft Corporation is not responsible in any way for the editorial policy or other contents of the publication.



Windows 8 Myths



Michael Otey

is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Email

A lot has been written about Windows 8 and how it's either Microsoft's biggest success or its worst failure since Vista. Admittedly some of this has been written by yours truly. However, I've come across a lot of statements that just don't jibe with my own experiences. Like most of you, at the current time, I don't have any touch-enabled hardware. So running Windows 8 is basically just like Windows 7. I have Windows 8 installed on several desktops and have been using it on a daily basis since its GA release in October 2012. I know how it works.

Most normal (non IT) people I know are interested in Windows 8. But when they see it and first try to use it they are confused and don't like it. The IT crowd catches on to it pretty quickly, but for the most part they say they see no advantage over Windows 7 (which by all accounts has become the new XP). Not unexpectedly, the exceptions are people who are ardent Microsoft supporters. Fortunately being an independent publication means that we can provide opinions that aren't colored by the Microsoft party line. Here are my thoughts about some of the myths that I've run into about Windows 8.

You might as well get used to Windows 8 because it's inevitable. Windows 8 is most certainly not any more inevitable than Windows Vista was. Like Windows Vista, Windows 8 is off to a slow start. But I expect that Microsoft is going to be coming out with an update that helps address some of main pain points in the initial release. So if you don't like Windows 8, just hold off, because a subsequent version is going to get better.

Windows 8 is unusable without a touch screen. Windows 8 is different from any previous version of Windows. At first it's confusing, and in my opinion in day-to-day use Windows 8 isn't as productive as Windows 7. However, Windows 8 is definitely very usable. While not as efficient as Windows 7, you learn how to cope with its differences.

Basically, I just wound up living on the desktop side and junking up my desktop with a zillion shortcuts to make up for the missing Start menu. Start8 or Classic Shell can also help make Windows 8 more livable.



Video

Michael Otey dispels some Windows 8 myths

Windows 8 is faster than Windows 7. Nope. Sorry, it's not. But it's not slower, either. To me, Windows 8 seems identical to Windows 7 in terms of speed. If there's any difference, I can't see it, and I'm looking. Maybe Windows 8 is faster if you're running on new, faster hardware, but then that's really the hardware. Right?

Windows 8 boots faster than Windows 7. This is true. Windows 8 boots faster than Windows 7, but so what? The last time I booted my desktop was well over a month ago. I doubt many people are spending a lot of time worrying about how long it takes their desktop to boot.

The new Start screen is better than the old Start menu. I've heard this myth from some Windows 8 supporters, but I just don't see it, at least not on non-touch devices. The old hierarchical Start menu provided quick access to all of your programs. The new flat Start screen requires paging to see what's there, and it doesn't show everything anyway. It also lacks jump lists and Recent Items options and quick

The IT crowd catches on to Windows 8 pretty quickly, but for the most part they say they see no advantage over Windows 7.

Most people are interested in Windows 8, but they are confused and don't like it when they first try to use it.

access to My Computer, Networking, the Control Panel, and Administrative Tools. To be fair, tiles can show you dynamic content, but gadgets did that as well.

Windows 8 is not for the enterprise. Microsoft might be marketing Windows 8 to the consumer (perhaps not altogether successfully because Microsoft is no longer a consumer-oriented company), but Windows 8 inherits all of the Windows 7 enterprise features such as full AD support, Bitlocker, Windows To Go, DirectAccess, BranchCache, and Applocker. Windows 8 can definitely be used successfully in the enterprise.

Old Windows programs won't run. Microsoft has only itself to blame for this one. It's true that the ARM-based Windows RT version of the OS will not run the old x86/x64 Windows programs. However, Windows 8 and Windows RT are really different things. The vast majority of x86 and x64 programs run just fine on Windows 8. I ran into a few devices that aren't supported, but all the programs and games I ran worked fine. Sometimes you have to wonder why Microsoft even named Windows RT "Windows." After all, the UI formerly known as Metro is designed to run one app at a time, not to have multiple windows open.

I have no doubt that touch is the way of the future, but I also know we're just not there yet. Microsoft designed Windows 8 with a bit too much eye on the future and forgot about where the rest of the world really is. I've shared some of the biggest myths about Windows 8 that I've come across. If you have some Windows 8 myths that you'd like to dispel, share your comments. ■

InstantDoc ID 145173

Office 2013 and Office 365

By the time you read this, Microsoft will have formally launched the new Office, which includes Office 2013 as well as new versions of the free Office Web Apps, the ever-expanding Office 365 online services, and hosted and on-premises versions of the Office servers. Although Microsoft will continue to offer Office products in traditional on-premises guise, the big news this time around is with the services and the products that will be delivered and treated as services. This isn't a subtle distinction, and it dramatically changes the products and how they're deployed and serviced going forward.

Office 2013

Given the sheer volume of Office-related products and services that Microsoft dumped on us in early 2013, you're forgiven for not being sure whether the traditional, locally installed Office applications and suites still exist. They do. They can be procured, deployed, and managed in all the traditional ways with which you're familiar. But individuals and—go figure—families have some very interesting new options with this release, which, thanks to a new Office 365 version described later in this article, can be purchased, deployed, and managed like an online service.

We'll get to that in a moment. For now, let's look at what's changed with the suites.

As before, Office 2013 provides multiple suites, each with an ever-increasing set of included applications. If you're a fan of this traditionally-installed software—or, perhaps more accurately, not a fan of software subscriptions—Microsoft has made one major negative change in Office 2013: All of the suites include just a single license and can thus be installed on only one Windows PC.

So although you can buy the low-end Office Home & Student 2013, which includes Word, Excel, PowerPoint, and OneNote 2013, multi-PC



Paul Thurrott

is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows, a weekly editorial for Windows IT Pro UPDATE, and a daily Windows news and information newsletter called WinInfo Daily UPDATE.

Email

Twitter

Website

installation rights are a thing of the past. Your $140 buys you just a single installation.

Next up the chain is Office Home & Business 2013. This suite includes all the applications from Office Home & Student, adds Outlook, and costs $219.99, again with just one PC license.

Up a level, there's Office Professional 2013. It includes all of the applications from Office Home & Business, plus Access and Publisher, and costs $399.99 per PC.

Most of the Office 2013 applications—Word, Excel, PowerPoint, Outlook, Publisher, and Access—can also be purchased individually for $109.99, although OneNote is $69.99. Businesses gain access to Office Standard 2013 and Office Professional Plus 2013, the latter of which adds InfoPath and Lync to the Office Professional application set, through volume licensing.

I've written a lot about Office 2013 on the SuperSite for Windows. One good place to start might be my series of Office 2013 feature focus articles, which I'll expand on over time.

Office 365

If you're familiar with Office 365, you know that Microsoft improved on its previous attempt at online hosted versions of Exchange, SharePoint, and Office Communications (the Lync predecessor)—called Microsoft Business Productivity Online Suite, or BPOS—and delivered a truly useful set of online services about 18 months ago. The initial Office 365 versions targeted businesses of various sizes and provided hosted versions of Exchange, SharePoint, and Lync.

I've held up Office 365 as proof that Microsoft could move quickly when it mattered. This service is a stunning example of the firm taking highly successful on-premises products and moving them to the cloud. My one niggling complaint, that Microsoft didn't have a free offering to rival the free version of Google Apps that most small businesses and individuals were using, was rendered moot in late 2012 when Google announced it was killing its free offering.

With this new Office wave, Office 365 soldiers forward and picks up a decidedly consumer-oriented version as well. Dubbed Office 365 Home Premium, this new version of Office 365 is an odd duck for several reasons. The most obvious reason is that it's Office 365 in name only: It is the only Office 365 version that doesn't offer access to hosted versions of Exchange, SharePoint, and Lync.

Instead, Office 365 Home Premium is aimed at households that have multiple PCs and devices and are looking to use Office 2013 on up to five of them. It's inexpensive—$99.99 per year or $9.99 per month—and comes with some extras—20GB of additional SkyDrive storage and 60 minutes of Skype world minutes each month, for starters—and the version of Office you get is analogous to Professional, making it a much better deal than any of Microsoft's business offerings. It's almost a no-brainer, especially for those IT pros with families who want to keep the work lights burning in the off-hours.

The trick to Office 365 Home Premium is that it assumes everyone using the service already has a Hotmail or Outlook.com account, SkyDrive, and Skype . . . which they do, since the one requirement this service has is that you must have a Microsoft account. But here's the thing: Thanks to the pliability of Office 2013, you can acquire the suite at home cheaply with Office 365 Home Premium, then configure it to use any number of SkyDrive and SharePoint or SharePoint Online accounts. And yes, you can mix and match. This makes the service even doubly more impressive, I think.

SharePoint 2013 and SharePoint Online

Looking at Microsoft's Office servers—and the hosted online services, which, in this version and going forward, are both more powerful and will be updated more frequently—I'm most interested in SharePoint. One of the firm's least heralded success stories, SharePoint is one of those servers—excuse me, services—that's immediately obviously useful, and now the online, hosted version has finally caught up to the on-premises version. As with the rest of Office, SharePoint now

can appeal to the entire customer gamut, from individuals (with Office 365 Small Business) to small businesses, to enterprises, government, and education.

SharePoint has Yammer integration now too, thanks to a 2012 purchase of the company and its technologies. Yammer expands on SharePoint's already impressive business-oriented social network functionality. But maybe the best aspect to this integration is that Microsoft has simplified the deployment and management of Yammer as well as the licensing costs: Yammer Basic Standalone is free and Yammer Enterprise Standalone is just $3 per user per month. If you're coming through the Office 365 business packages, pricing starts at $8 per user per month (for the entire suite of functionality).

Using SharePoint Online in Office 365, I'm struck by a few changes. The service picks up a more streamlined ribbon-based UI that's akin to what you'll see in Office 365, and the layout and presentation of various interfaces is cleaner and, dare I say it, more "Metro-like." But it's not just a pretty face. There are some interesting functional changes too.

In this revision, Microsoft has replace SharePoint Workspace with the horribly misnamed SkyDrive Pro. If you're familiar with the SkyDrive desktop application, SkyDrive Pro is identical except that it connects to your SharePoint document storage on the back end instead of to the consumer-oriented SkyDrive service.

That is, SkyDrive Pro integrates SharePoint directly into your PC's file system so that you can interact with your SharePoint content just as you do with the documents in My Documents. In fact, many will simply point My Documents to this SkyDrive Pro folder structure and be done with it.

In the same way that you can mix and match SkyDrive and SharePoint in the Office applications, you can also have both SkyDrive desktop applications and SharePoint SkyDrive Pro applications installed on your PC. They will sync to your personal (SkyDrive) and work (SharePoint) data stores without any issues or conflicts. Note,

however, that you can have only one instance of each, whereas the Office applications let you integrate any number of SharePoint repositories and SkyDrive accounts.

The biggest change to SharePoint, perhaps, is the new application model, which is shared with Office 2013 applications. Code-named Agave, it provides extensibility of SharePoint using HTML5 technologies—including JavaScript and CSS—so you can deploy your own apps or browse a new Office App Store to find apps from third parties.

If you're familiar with the extensibility model used in previous SharePoint versions, you know that SharePoint Online lagged behind on-premises versions fairly significantly because of the different architectures. But most of these issues have been resolved.

Also new to this release is a set of mobile apps aimed at Windows 8, Windows RT, Windows Phone, and iOS (Apple iPad and iPhone). These include a news feed app for keeping up with the documents and other items you're following in SharePoint—essentially a native version of SharePoint's enterprise portal functionality—and a SkyDrive Pro app that will let you browse your own documents from mobile devices. Microsoft plans to expand support for these apps to Android in the future, too, but for now Android users are served by mobile web experiences.

Office in a Nutshell

The products and services I've mentioned here are just the tip of the iceberg, and much of what I've related is, of course, consumer focused. This is by design: Office remains the productivity workhorse you've used for years. But the big change in this release, I think, is the blurring of the lines between work and home and between service and on-premises product. Microsoft's greatest strength heading into the cloud computing age is that it alone can offer hybrid solutions that bridge the gap between the past—on-premises servers, locally installed software—and the future—cloud services, with data synced to ultra-portable mobile devices.

Taken alongside other recent moves at the company, such as the release of Windows 8 and Windows RT, the latter of which runs on an entirely new class of software, these new Office solutions point the way to the future. Even cloud doubters should take note of the fact that Microsoft's solutions, uniquely, don't actually require you to give anything up to embrace this new, more efficient way of doing things. Firms like Google, which sees everything solely through the lens of the Internet and web services, and Apple, which pretty much makes just expensive consumer electronics, will never offer this choice.

This is important because Microsoft sees itself as a devices and services firm. Oddly enough, this is perhaps best exemplified in the new Office, which, incidentally, will expand later in 2013 to embrace rival mobile platforms including iOS and Android, I'm told.

Office isn't just emblematic of Microsoft's aspirations but is rather the almost literal embodiment of Microsoft. This is the future of the company—and for those of us who support it and its products, and the people who use them, the new Office is the clearest sign yet that Microsoft intends to flourish in this ever-changing market.

Windows 8, Windows RT, and Windows Phone 8 are of course important and innovative in their own ways. But Office is successful on an entirely different level.

But don't take my word for it. Office 2013, Office 365, and the new Office services and servers are all available now for your evaluation. Whether you've been skipping Office releases or not, this is one version of Office you're going to want to consider. ■

InstantDoc ID 145206

Meet Set-ADUser, an All-Purpose Hammer

It's the ultimate tool for Active Directory account tweaking

In "3 PowerShell Account Tweaks," I continued my discussion of Active Directory (AD) "hammers"—PowerShell cmdlets that don't just find users that meet a particular criterion (what I've called the "filters") but also accomplish something, such as unlocking an account. This month, I want to introduce you to the ultimate tool of AD account tweaking: *set-aduser*.

Set-aduser basically looks like

```
set-aduser -identity IDinfo -changeparameters
```

where *IDinfo* is—like *get-aduser*'s *-identity* parameter—an object's samaccountname, distinguished name (DN), object GUID, or SID. The *-changeparameters* option refers generically to many parameters that can change dozens of AD attributes such as title, description, and so on. For example, to change the display name of an account with the samaccountname JulesM to Julie Marsella, you'd type

```
set-aduser julesm -displayname "Julie Marsella"
```

The AD PowerShell folks included a lot of attribute-specific parameters, like *-Company, -Givenname, -description*, and others, so you'll probably find that *set-aduser* already has a built-in parameter that matches what you want to change. Most of them take simple strings, so you can change a bunch of attributes all in one shot, as in



Mark Minasi

is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 30 books, including *Mastering Windows Server 2008 R2* (Sybex). He writes and speaks around the world about Windows networking.

Email

Twitter

Website

```
set-aduser MartinT -description "Debugger" -Initials "R"
  -surname "Thomas"
```

As is often the case, the AD PowerShell team has made our lives a bit easier in a few ways. For example, specifying an account's Manager value requires a complete DN in most tools, but that's not the case here. Thus, if JulesM were MartinT's manager, then the command

```
set-aduser MartinT -manager JulesM
```

would let you tell that to AD (rather than *-manager "cn=julesm,cn=users,dc=bigfirm,dc=com"* or something like that).

Similarly, you might know that the AD attribute name for someone's last name is *sn*, which you probably know is a shortening of *surname*. That has always seemed odd to me because the AD attribute for what Americans would call a first name is *givenname* and it's completely spelled out, so why is the last name attribute *sn* rather than *surname*? The AD PowerShell folks have, however, made our lives easier by creating a sort of "synthetic" attribute called *surname* rather than *sn*. That does make changing someone's last name a bit odd if you're AD-savvy, because typing

```
set-aduser MartinT -sn "Thomas"
```

will get you an error, whereas

```
set-aduser MartinT -surname "Thomas"
```

works just fine. And that's not the only case of a "synthetic" attribute. You might recall that LastLogonDate is a godsend if you're trying to figure out who hasn't logged on in a while. The AD space for an email account is called *mail* inside AD, but you need to use *-emailaddress* rather than *-mail* to change an account's email address.

What about custom AD attributes? How can you set a value of an AD attribute that an application added to AD—like, say, *shoesize*? You can change any arbitrary AD attribute or attributes with *-replace*:

```
set-aduser identifier -replace @{attributename="newvalue";
  "attributename="newvalue"...}
```

So, to set Martin's *userprincipalname* and *givenname*, you'd type

```
set-aduser MartinT -replace @{userprincipalname=
  "martint@bigfirm.com";givenname="martin"}
```

Note that when you're using *-replace*, the attribute names must match their internal AD values, so to set Martin's email address and manager, you'd have to type the internal AD attribute name (*mail*) and specify the manager's name as a DN, as in

```
set-aduser MartinT -replace @{mail="martint@bigfirm.com";
  manager="cn=julesm,cn=users,dc=bigfirm,dc=com}
```

Set-aduser lets you clear any existing value with *-clear*, as in

```
set-aduser MartinT -clear mail
```

And again, *-clear* needs the internal LDAP names of the AD attributes. Some AD attributes allow more than one value, as is the case with *othermobile*, and can be set with *-add*, as in

```
set-aduser MartinT -add @{othermobile="+1724333-5544"}
```

You could then add as many more phone numbers as you wanted, and AD would store them for you. You could then see them with the *get-aduser* command, as in

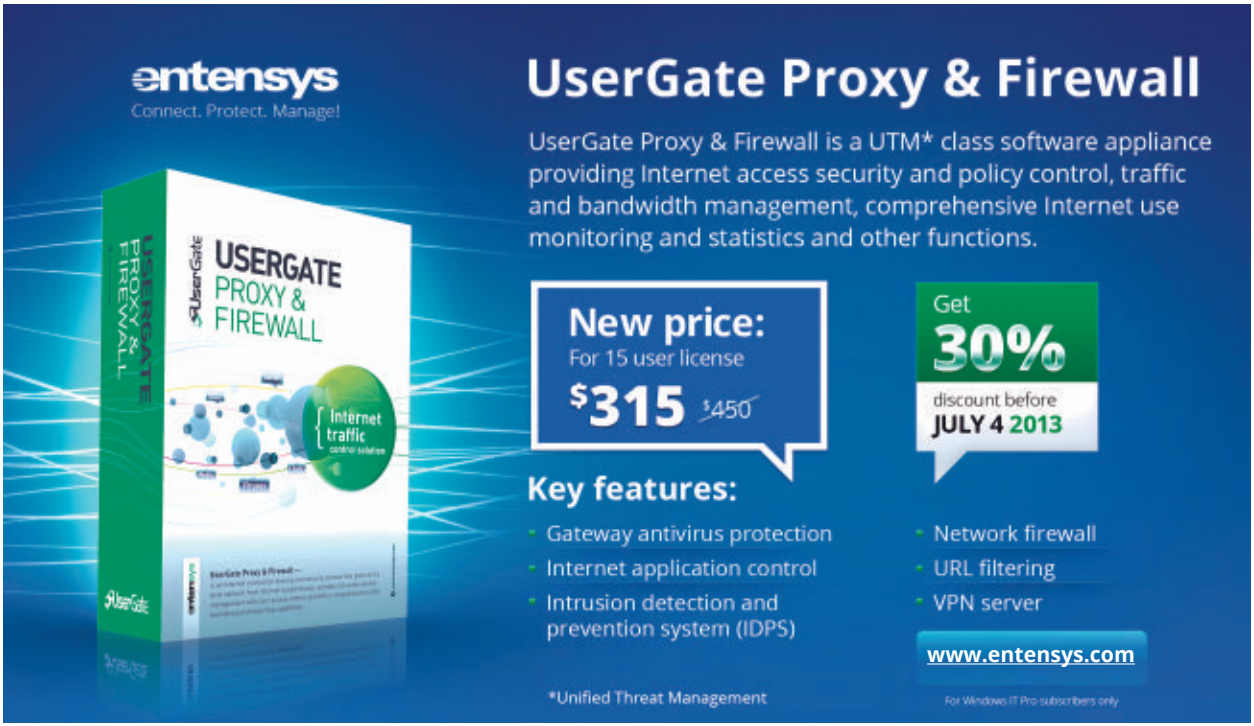
```
get-aduser MartinT -pr othermobile | select othermobile
```

Rounding out the set of commands begun with *-replace, -clear*, and *-add*, there's *-remove*, which removes an item from a list. To remove that first phone number from Martin's *othermobile* list, you'd use

```
set-aduser MartinT -remove @{othermobile="+1724333-5545"}
```

Set-aduser gives you a finely tuned ability to modify AD attributes. We'll see more of that next month! ■

InstantDoc ID 145115



New Features in Office 2013

Multiple new features make Office 2013 stand apart from earlier versions of Office

Microsoft released so many new products in 2012 that it was easy to overlook the latest release of the flagship Office product. Office 2013 was released to manufacturing on October 11, 2012, and was released for general availability on January 29, 2013. What makes Office 2013 different from the preceding versions of Office? A lot! Let's look at the top 10 new features in Office 2013.



Michael Otey

is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Email

1 Windows 8 touch support

Without a doubt, the biggest change in Office 2013 is support for the new Windows 8 touch screen interface. Although the Office 2013 UI is designed primarily for operation with a mouse and keyboard, it also offers support for touch. Click the Touch Mode button on the Quick Access Toolbar and the Office Ribbon spreads the Office 2013 icons apart for easier touch access. On touch-enabled hardware, gestures such as swiping with your fingers let you scroll and pressing with your fingers selects items.

2 Subscription-based pricing

Two editions of the Office 2013 family—confusingly named Office 365 Home Premium and Office 365 Small Business Premium—are sold as subscriptions (not a standard retail license), making them more affordable, but you must pay every year to continue using the software. Office 365 Home Premium goes for $99.95 per year and includes Word, Excel, PowerPoint, Outlook, OneNote, Publisher, and Access, plus 20GB of SkyDrive storage and 60 minutes of Skype per month. Office 365 Small Business Premium costs $149.95 per year and adds Lync, InfoPath,

hosted Exchange Server, 25GB mailboxes, 10GB of storage for the organization, and 500MB of SharePoint storage per user.

3 New pricing for retail editions

The Office Home and Student edition is the basic edition of the retail Office 2013 lineup. The Office Home and Student edition costs $139.99 and includes Word, Excel, PowerPoint, and OneNote. The Office Home and Business edition costs $219.99 and adds the Outlook application. The top of the retail lineup is the Office Professional edition, available for $399.99; it includes Access and Publisher.

4 Multiple-PC support

With Office 2013, the traditional software-based license offers no multicopy discount as Office 2010 did. However, the new subscription-based licensing covers up to five devices on a single license. This multiple-device support could be especially attractive to home and small business users.

5 Color-coded Start screens

The Office 2013 applications feature new color-coded Start screens. Each Start screen is colored to match its application icon. For instance, the Word Start screen has a blue theme, Excel is green, and PowerPoint is red. The new Start screens display a list of recent documents, a Getting Started tour, a blank document, and the application's templates.

6 Integrated SkyDrive

The Office 2013 programs provide seamless integration with SkyDrive. The Office 2013 Account Configuration page lists your Connected Services. You can include your SkyDrive authentication information and Office 2013 will connect and authenticate when you start an Office 2013 application. Your SkyDrive account details are displayed in the top-left corner of the application, and your default Save location is your SkyDrive.

7 Office on Demand

Another useful cloud addition to Office 2013 is Office on Demand. All Office 2013 users can access the web-based versions of the Office 2013 applications they have licensed—even on PCs where no version of Office 2013 is installed. Office on Demand works with Windows 7 and Windows 8 PCs and uses Microsoft's Click-to-Run technology to stream the applications to the end user's device. Office on Demand can be used for Word, Excel, PowerPoint, Access, Publisher, and InfoPath. Check out Paul Thurrott's "Office 2013 Feature Focus: Office On Demand" for more information.

The biggest change in Office 2013 is the support for the new Windows 8 touch screen interface.

8 PDF editing in Word

One long overdue feature is Word 2013's ability to edit PDFs. In Word 2010, you could save a Word document as a PDF, but you couldn't edit PDFs directly. The new Word 2013 lets you open PDF files, edit them, and then save them as a .doc, .docx, or .pdf file.

9 Lync 2013

Office 2013 includes the new version of the Lync communications platform, Lync Server 2013. Lync replaced the older Office Communications Server (OCS). Lync 2013 can do IM and group IM, as well as audio and video conferencing. Lync is integrated into other members of the Office 2013 suite, including Outlook and OneNote. Lync 2013 also features integration with Skype.

10 Windows RT support

Microsoft includes an ARM version of the Office 2013 suite on the distinctly non-x86 Windows RT platform, giving Windows RT the possibility of actually being a useful business device. The Windows RT Surface tablets include Office 2013 Home and Student edition, which contains Word, Excel, PowerPoint, and OneNote. Documents are fully interchangeable with other x86 versions of Office 2013. ■

InstantDoc ID 144940

Virtualized Infrastructure Provides Flexibility for State Department

NWN Corporation helps clients solve business problems through technology. The company provides clients with a complete range of technology solutions and services available across various delivery models. The solutions and services include collaboration, custom applications, executive intelligence, networking and data center, security, workspace and mobility, managed services, professional services and staff augmentation services. NWN's delivery models provide customers with the flexibility to determine if as-a-service or customer owned, hosted or on premises, or hybrid will best suit their environment.

NWN has more than 550 employees in 14 offices in the US and one in China. The company has been recognized as one of the fastest growing, privately held IT solutions companies in the country, ranking fifth in Inc. *magazine's annual survey. NWN is privately held and woman-owned.*

NWN's clients include private and public sector organizations in almost every line of work. It provides solutions to universities, PreK-12 districts and schools, financial institutions, manufacturers, hospitals, retailers, professional service providers, and state and local government agencies.

Moving to a cloud-based or virtualized infrastructure is no simple task. Even when you can build a brand new system from the ground up, finding the skill set necessary to move business workflow to a virtualized or service-based approach can be difficult.

That's why when a major Department of Social Services (DSS) decided it was time to migrate from its mainframe backend, modernize its infrastructure, and move its clients to Windows 7, the department called on NWN Corporation, an HP-Microsoft Frontline Partner of the Year 2012. NWN took the lead on moving the DSS into a new state federated datacenter with a goal of maximizing the organization's existing investment in Microsoft server and collaboration technologies. NWN's collaborative approach with the client IT team, along with its detailed planning and analysis—prior to getting in the trenches and rebuilding the client infrastructure—are all key parameters in the long-term success of NWN and its clients.

Keeping that goal in mind, NWN built a virtualized datacenter infrastructure running Microsoft Windows Server 2008 Datacenter

Edition with Hyper-V on HP C7000 BladeSystem servers and HP networking hardware. To maximize networking and storage flexibility, NWN used HP Virtual Connect technology.

The Virtual Connect technology, which links the BladeSystem servers and a SAN storage environment that includes HP 3PAR storage systems, allows servers to be added, moved, and changed within the BladeSystem domains without impacting the access of those physical and virtual servers to LAN and SAN resources within the domain. This gave NWN the ability to configure hardware, storage, and networking resources so that the new datacenter could update, deploy, and provision as necessary.

On the software side, NWN modernized an existing Microsoft SharePoint Server and SQL Server installation to take advantage of the new hardware and virtualization infrastructure. Custom .NET development delivered a customer-optimized solution. Microsoft System Center 2012 also came into play with Configuration Manager, Operations Manager, Virtual Machine Manager, and Forefront Identity Manager all playing a role in allowing the customer to better leverage its investment in Microsoft technologies.

To make the migration of the end user computers to a new desktop operating system a more controllable and manageable operation, Microsoft System Center Configuration Manager 2012 became the backbone in the rollout of Microsoft Windows 7 clients to HP desktop hardware throughout the customer end user environment. NWN was able to install the approved client configuration on each machine and properly implement Microsoft BitLocker data protection throughout the enterprise. The migration path for client IT needed to maintain the security and manageability of the devices and infrastructure as new technologies replaced old. And it needed to take advantage of the explosion of IT- and user-provided devices, along with the growing technical skills of the average user.

innovation³
frontline partner of the year

Microsoft

To build the proper infrastructure for a statewide deployment of the migration process, DSS field offices throughout the state had managed Microsoft Hyper-V virtual machine installations to facilitate upstream and downstream deployments of operating systems and applications. There was also an effort to make greater use of business intelligence as part of the business process. As the amount of data continues to grow, being positioned to make use of that ever-increasing data store builds a platform for future successes.

These processes are all part of what NWN calls “the Power of NOW,” an approach that allows a client to streamline its processes and use familiar tools and applications. With this approach NWN was able to leverage existing technologies to build an infrastructure with greater flexibility and growth potential. ■

A New Approach to Identity Management

Managing the inside from the outside



Sean Deuby

is technical director for *Windows IT Pro* and *SQL Server Pro* and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

Email

Twitter

Identity and Access Management (IAM) has always been a complicated subject. The basics haven't changed much: Who are you? What should you have access to? The third question—How do you prove the accuracy of your answers to the first two questions?—is a relative newcomer compared with simple account provisioning, but it has grown dramatically in importance over the past 10 years, thanks to regulatory requirements such as Sarbanes-Oxley as well as an increase in malware and cybercrime. With the advent of cloud-based identity management as a service (IDaaS) offerings, there are more ways to get these answers from both on-premises applications and the cloud services your users subscribe to. These solutions allow you to rearrange the puzzle pieces of identity management into different configurations to provide varying types of functionality. This month, I'd like to look at where different types of solutions fit into your existing identity management architecture, and examine the emerging puzzle called "from the cloud." Collectively, Gartner has christened these solutions as *identity bridges* because they bridge your on-premises identity systems with cloud systems. I wrote about this topic in more detail in "Building Your Identity Bridge to the Cloud."

Cloud Integration

Before I dive into the different identity management architectures you can use, single sign-on (SSO) to a cloud service clearly requires that the user attempting to use the cloud service be authenticated. This is best accomplished with federation between the identity provider (your enterprise and Active Directory—AD) and the service provider

or relying party (the Software as a Service—SaaS—provider or other cloud service). What's not immediately obvious is that, even though federation allows a user to authenticate at a cloud service with an on-premises AD password, practically all SaaS providers require you to have a local account before you can authenticate. There are a number of reasons for this requirement, but the practical result is that for every one of your users who wants to use the provider's service, a shadow account (of his or her AD account) must exist on the SaaS provider.

Therefore, in addition to an authentication puzzle piece, there also has to be a puzzle piece that handles cloud service account provisioning and, ideally, de-provisioning. Cloud service provisioning is an active topic in itself; for now, just know that it's something that needs to get done as part of working with a cloud service.

The new breed of cloud-based identity management solutions has varying degrees of integration into an existing on-premises identity infrastructure (e.g., AD, an HR system). Some of these solutions are designed to bolt on to your existing identity management environment with as little impact as possible to on-premises identity stores and lifecycle processes. These are IDaaS systems such as Symplified, Okta, and OneLogin. These usually have an on-premises component such as a hardware device, virtual machine (VM), or simply a service running on an existing server that performs several important functions between your company and the IDaaS provider.

First, this local IDaaS component provides some kind of account synchronization between your on-premises identity (e.g., AD) and the cloud identity service to populate the service with your company's authorized user accounts. A typical method is to synchronize with certain OUs or security groups, populating the IDaaS provider's account database with the OUs' or groups' membership. This method is known as directory synchronization. Other methods are available, such as SAML just-in-time provisioning or System for Cross-domain Identity Management (SCIM). Second, the on-premises IDaaS component also

provides a federation gateway between your company and the IDaaS provider. In contrast to the next example, this is a dedicated connection just between you and the provider, and to my knowledge it can't be extended to any other service provider. Third, these on-premises components act as reverse proxies for the identity service and might also provide auditing and reporting capabilities.

It's worth noting that IDaaS solutions don't necessarily require any integration with an existing on-premises identity infrastructure; from their perspective, life is much simpler if you simply create, store, and manage your identities entirely within their offering. Maintaining all these identities in the cloud rather than on premises is a big step for companies with any size of on-premises identities, but it's very appealing to startups that have no existing infrastructure to take apart.

Going Deeper

The next type of identity bridge requires a deeper level of integration with your on-premises identity management environment. This type is a general-purpose, on-premises federation service that can provide connections to multiple service providers. It's a traditional enterprise application that you deploy and maintain, and you must establish a federated trust to every cloud service provider you want to have SSO with. Ping Identity's PingFederate and Microsoft's Active Directory Federation Services (AD FS) are examples of this federation capability. This type of solution doesn't necessarily take care of the account provisioning requirement; how this gets done depends on the cloud service that the identity provider is connecting to. For example, Office 365 requires a directory synchronization component.

Moving more deeply into on-premises identity management integration, many vendors in the traditional enterprise identity management market are adding cloud-based services to complement their existing offering. For example, Radiant Logic, a well-known virtual directory service provider, now also offers an integrated federation service. Centrify, a market leader in the on-premises AD bridge solution

(which allows non-Windows systems to use AD), has expanded to offer its own cloud-based SSO to SaaS providers.

These are all what Gartner calls "to the cloud" scenarios: Identities are created, updated, and managed within the enterprise and are extended from these on-premises identity systems to relying parties in the cloud, such as Salesforce, Google Apps, and Concur. A newer breed of identity management solutions, known as "from the cloud," takes cloud involvement a step further by centralizing both on-premises identity lifecycle management and cloud identity management in a cloud-based (rather than on-premises) management portal.

This puzzle piece arrangement is a substantial conceptual shift for IT, because not only are you managing your new cloud-based capabilities from the cloud (which the Symplifieds, Oktas, and OneLogins are already doing), you're also moving management of on-premises identity stores—one of the bedrock pieces of IT infrastructure—to the cloud. Identropy's SCUID Lifecycle is the first product of this type I'm aware of; the company describes it as identity lifecycle management and governance for the hybrid enterprise because it manages both on-premises and cloud identity equally.

In this architecture, the on-premises component VM (which Identropy calls the identity connector for the enterprise—ICE) has elevated rights to a wide variety of on-premises identity stores such as AD or SAP and, on direction from the cloud-based Lifecycle service, performs create/read/update/delete (CRUD) operations on them. It also manages account provisioning and appropriate de-provisioning (a thornier issue than simply provisioning accounts) to other cloud services. Identity administrators—and end users if you've configured it—use the SCUID Lifecycle web portal to perform their management tasks.

Why might you consider such a solution? First, it would probably save you a lot of money. Traditional on-premises identity management systems are expensive to purchase, deploy, and maintain in both headcount costs and annual maintenance fees. SCUID Lifecycle charges a simple per-user fee that drops rapidly with the number of

users. To keep implementation costs down, SCUID has created a set of templates that it believes describes the vast majority of on-premises identity management configurations, and it charges a one-time setup fee to create a semi-custom configuration for your identity management environment based on one of these templates. SCUID maintains it is also very straightforward in telling a potential customer whether it simply won't fit into one of its configuration templates.

Another reason to think about a solution like this is that it should be easy to work with. On-premises systems have complicated and user-unfriendly interfaces—especially for end users. The trend toward simplifying the UI is a good one, and SCUID Lifecycle's is extremely straightforward. (I also give extra-credit points to Identropy for using "freaking suck!!" to describe traditional identity management systems' UIs in its product's web intro.)

A Question of Comfort

Are you instinctively uncomfortable with this "from the cloud" solution? You don't like having your identity management hosted off premises, potentially more exposed and more dependent on external factors? Well, if you lose your Internet connection, you'll lose all your SaaS applications and the ability to perform integrated identity management, but you can still manage identity through local interfaces (e.g., Active Directory Users and Computers), and the ICE VM tracks and queues up changes to integrate into the Lifecycle system when the connection becomes available again. The real choice is cost savings and time to value versus your acceptable level of risk associated with managing identity using any outside entity.

Identity management technology has been re-energized by all the possibilities the cloud computing model affords us, and a whole market of identity service providers has materialized in the past few years to take advantage of these possibilities. Whether the market will embrace all of them remains to be seen. ■

InstantDoc ID 145141

How Windows Server 2012 Eases the Pain of Kerberos Constrained Delegation, Part 1

Let's talk authentication—specifically, Kerberos constrained delegation. But first, if you're new to Kerberos or need a quick refresher, I would suggest that you read the Ask the Directory Services Team blog posts "Kerberos for the Busy Admin" and "Understanding Kerberos Double Hop" to get up to speed on the terminology and concepts contained throughout this article. Part 1 of this article describes the benefits of using Kerberos constrained delegation with Windows Server 2012 over earlier versions of Windows Server. Part 2 will provide a technical walkthrough of how Kerberos constrained delegation works in Server 2012.

What Is Constrained Delegation?

Constrained delegation lets you limit the back-end services for which a front-end service can request tickets on behalf of another user. A common example is the web-browser-to-IIS-to-SQL-Server scenario. In this scenario, a user navigates to a web-based reports server hosted on Microsoft IIS, which retrieves data using an authenticated connection to a Microsoft SQL Server system. The IIS server needs to authenticate to the SQL Server system on behalf of the user. Through Kerberos delegation, the IIS server (i.e., the front-end service) can request a service ticket for any service (i.e., back-end service)—not just SQL Server—on behalf of the user. This means that the IIS server can essentially authenticate on behalf of the user to SQL Server, a file share, or a web service. Using constrained delegation, you can limit the IIS server (the front end) so that it can authenticate the user only to SQL Server (the back end) and no other service or application.



Mike Stephens

is a senior support escalation engineer with Microsoft Commercial Technical Support. He is a Microsoft Certified IT Professional (MCITP-EA) and a Microsoft Certified Trainer (MCT). He recently authored and delivered Windows Server 2012 Distributed Systems Security training for Microsoft Commercial Technical Support. He is a contributor to the Ask the Directory Services Team blog.

Email

Kerberos constrained delegation has been a part of the OS since Windows Server 2003. It requires you to configure an allow list of service principal names (SPNs) on user or computer objects in Active Directory (AD). You add the list of SPNs that represent the back-end services to which a front-end service is allowed to request tickets on behalf of the user to the ms-DS-Allowed-To-Delegate-To attribute of the principal under which the application or service on the front-end server runs. In the previous example, the front-end service is IIS and the back-end service is SQL Server. To constrain the delegation for IIS, you would add SPNs for the SQL Server instances running on the SQL Server system to the ms-DS-Allowed-To-Delegate-To attribute on the IIS computer account in AD—or the user account running the IIS application pool. This model constrains the front-end service to only request service tickets that are listed in the ms-DS-Allowed-To-Delegate-To attribute. The downside of this delegation model is that it relies heavily on SPNs.

Service Principal Names

SPNs are difficult to manage. Although they're simple in concept, SPNs can cause a significant amount of frustration, stemming from unique constraints associated with using them.

Kerberos uses SPNs to identify the security principal responsible for running an application or service. This enables the Key Distribution Center (KDC) to encrypt tickets and keys with the correct hash so that the security principal (running the service or application) can decrypt the service ticket upon receiving the AP_REQ. This design requires that SPNs registered on security principals be unique for the AD forest. An SPN registered on multiple security principals will cause authentication to fail.

Constrained delegation appears to contradict the basic rule of registering a duplicate SPN; however, this is only in appearance. The KDC doesn't look at the ms-DS-Allowed-To-Delegate-To attribute when trying to map an SPN to a security principal. Therefore, the unique SPN

requirement is limited only to values in the servicePrincipalName attribute. To constrain the delegation of a service or application, you must list the service's SPNs on the security principal that runs the application on the front-end server.

Managing the number of SPNs, knowing when and where to register them, and avoiding duplicates is cumbersome. This makes constrained delegation difficult to implement, maintain, and troubleshoot.

Point of Delegation

Constrained delegation is a model that controls delegation on the front-end server. Most delegation models manage the point of delegation closest to the resource (i.e., on the back end). Implementing delegation on the front end removes control from the resource administrator and places it on the administrator of the front-end server (and application). This model prevents the resource administrator from managing access to the resource. The current model requires domain administrative privileges to modify the ms-DS-Allowed-To-Delegate-To attribute, thus adding more administrative overhead to the management of constrained delegation.

Scope of Delegation

Scope of delegation refers to the limit to which the delegation extends from the front-end server to the back-end server. The current constrained delegation model scope is limited to the domain, meaning that the security principal under which the application or service runs can forward constrained delegated tickets only to an application or service running under a security principal in the same domain. You can't use constrained delegation across domain or forest trusts.

What Windows Server 2012 Brings

Server 2012 introduces a new kind of Kerberos constrained delegation that addresses many of the shortcomings that exist with the

previous constrained delegation model. The new implementation of constrained delegation removes the dependencies on SPNs for delegation configuration, removes the need for domain administrative privileges, enables the resource administrator to own the delegation experience, and increases the scope of delegation.

Constrained delegation in Server 2012 introduces the concept of controlling delegation of service tickets using a security descriptor rather than an allow list of SPNs. This change simplifies delegation by enabling the resource to determine which security principals are allowed to request tickets on behalf of another user.

Figure 1 shows a sample scenario. A server in Domain A runs an IIS application. The security principal under which the IIS application's AppPool runs has the SPNs registered for the front-end service or application (HTTP/app1.contoso.com). These SPNs allow the user to authenticate to the front-end server using normal Kerberos authentication.

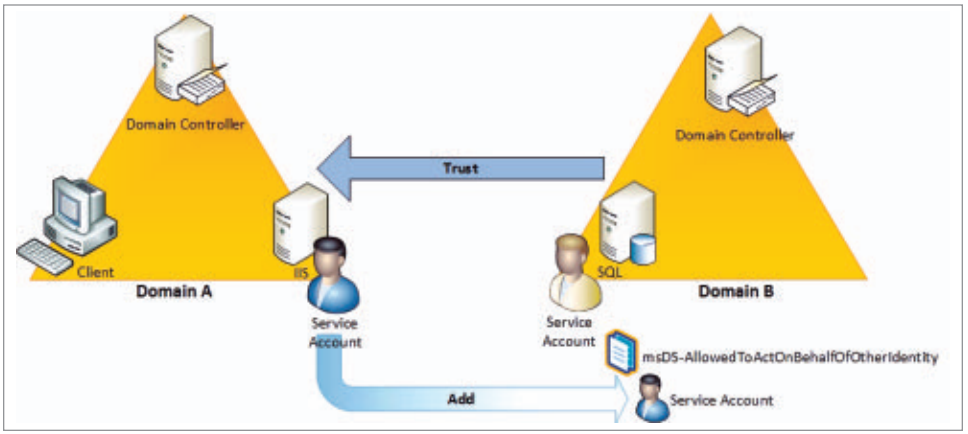


Figure 1
Constrained Delegation in Server 2012

The application retrieves data from a back-end server in Domain B running SQL Server. The security principal running the SQL Server service has the SPNs registered for SQL Server and SQL Server instances. Again, this configuration is normal to enable Kerberos authentication. The KDC in the domain hosting the security principal

running SQL Server receives a Service-for-User-to-Proxy (S4U2Proxy) Ticket Granting Service (TGS) request from the IIS server on behalf of another user. The KDC reads the security descriptor stored in the msDS-AllowedToActOnBehalfOfOtherIdentity attribute on the security principal running the SQL Server service and performs an access check using the identity under which the IIS Application Pool runs. A successful access check allows the authentication process to continue, whereas an unsuccessful access check fails the authentication attempt.

Resource-based constrained delegation functions correctly regardless of domain functional level and number of domain controllers (DCs) running a version of Windows Server prior to Server 2012, provided you have at least one Server 2012 DC in the same domain as the front-end server and one Server 2012 DC in the domain hosting the back-end server. When the domain is a hybrid domain (both Server 2012 DCs and DCs running an earlier version of Windows Server), then Windows 8 and Windows 2012 computers ensure they use a Server 2012 DC to use resource-based constrained delegation by deliberately locating a Server 2012 DC.

Requirements

The new implementation of Kerberos constrained delegation has the following requirements:

- Server 2012 KDCs must reside in the front-end account domain
- Server 2012 KDCs must reside in the back-end account domain
- The front-end server must run Server 2012

Server 2012 KDCs are required for this feature because these are the only KDCs that know how to return referred S4U2Proxy requests and use the new msDS-AllowedToActOnBehalfOfOtherIdentity attribute on the service account. The front-end server requires Server 2012 because the version of Kerberos on these servers understands that it must chase S4U2Proxy referrals to trusted domains and forests.

Management

You manage Server 2012 Kerberos constrained delegation using Windows PowerShell. Use the following Windows PowerShell cmdlets to manage constrained delegation. Typically, you'll want to use the Get-ADUser, Get-ADComputer, or Get-ADServiceAccount of the principal running the front-end service and pass that principal object as the argument value to the -PrincipalsAllowedToDelegateToAccount argument.

```
Set-ADComputer computerName
  -PrincipalsAllowedToDelegateToAccount
  principal1, principal2, ...
Set-ADUser userName
  -PrincipalsAllowedToDelegateToAccount
  principal1, principal2, ...
Set-ADServiceAccount serviceAccountName
  -PrincipalsAllowedToDelegateToAccount
  principal1, principal2, ...
Get-ADComputer computerName -Property
  PrincipalsAllowedToDelegateToAccount
Get-ADUser userName -Property
  PrincipalsAllowedToDelegateToAccount
Get-ADServiceAccount serviceName -Property
  PrincipalsAllowedToDelegateToAccount
```

Stay Tuned for More

This article identifies the challenges IT pros face when implementing Kerberos constrained delegation. Server 2012 provides a compelling answer to these problems by introducing resource-based Kerberos constrained delegation. In Part 2 of this series, I'll provide a more in-depth analysis of how resource-based constrained delegation works and look at the flow of authentication that's exchanged between computers running Server 2012. ■

InstantDoc ID 145167

FAQ

Answers to Your Questions

Q: How do I enable Office 2013 touch mode for easier use on my tablet or slate?



John Savill



Jan De Clercq

A: Office 2013 features a touch mode that increases the space between commands, making the application more touch friendly. To enable, select Touch Mode from the Quick Access Toolbar in Office 2013, then enable the Touch Mode via the new button that's displayed (see Figure 1). When enabled, Touch Mode spreads out the icons. It's great for use on tablet or slate-type devices.

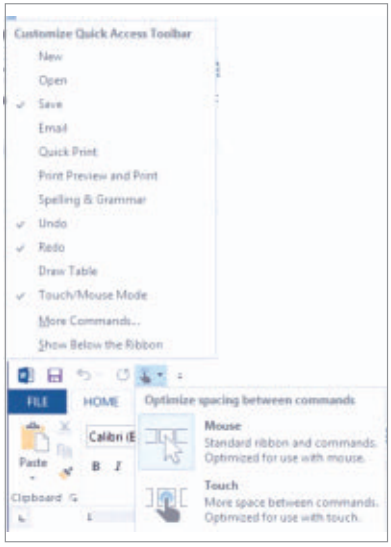


Figure 1
Office 2013 Touch Mode

—John Savill

Instant Doc ID 144594

Q: Can we use IIS Shared Configuration to share SSL configuration data and certificates between different web servers?

A: Yes, this type of sharing is possible in IIS 8, which is bundled with Windows Server 2012, through the new Centralized SSL Certificate Support feature. Microsoft introduced the IIS Shared Configuration feature in Windows Server 2008 to let multiple web servers share the same configuration that's stored on a central file share. Changes to the central master configuration file are

automatically propagated across the different web servers pointing to the shared configuration store.

Centralized SSL Certificate Support lets web server administrators store and access SSL/TLS X.509 certificates centrally on a file share. This location can be the same share that's used by the Shared Configuration feature; see the Microsoft article "Shared Configuration" for more details about how to set up this feature.

Centralized SSL Certificate Support eases SSL/TLS certificate management on web servers. Simple tasks such as renewing a certificate don't have to be repeated on every web server. Also, adding a new server to a web farm and SSL-enabling it becomes much easier.

Centralized SSL Certificate Support is an optional feature of IIS 8 that isn't installed by default. You can install it from Windows Server Manager by selecting Centralized SSL Certificate Support in the Security node of the Role Services for the Web Server Role.

You can configure Centralized SSL Certificate Support from a new configuration item called Centralized Certificates that's located in the Management section underneath the server node in the IIS Manager. Double-click the Centralized Certificates item and select Edit Feature Settings from the Actions pane to open the Edit Centralized Certificates Settings configuration screen that Figure 2 shows.

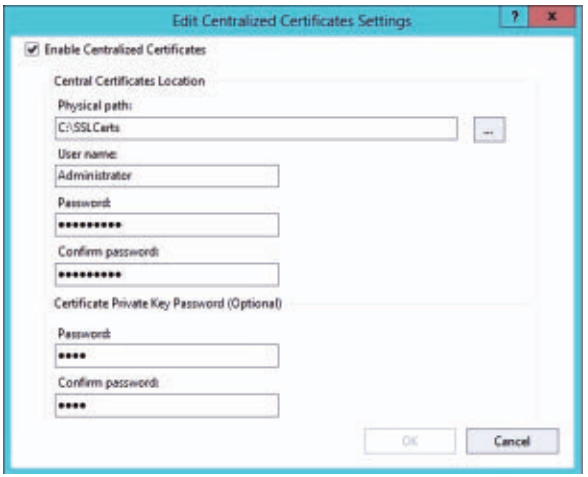


Figure 2
Edit Centralized Certificates Settings Configuration Screen

From this configuration screen, you can enable or disable Centralized SSL Certificate Support, enter the path to the central configuration share, enter the credentials that are needed to access the share, and—for PKCS #12 certificate files (*.pfx) that are protected with a

password—configure the password that's needed to unlock access to the certificate in the PKCS #12 file.

After you configure Centralized SSL Certificate Support, you can use the Centralized Certificates item to browse the certificates in the central share. An interesting feature is the ability to group the certificates by expiration dates. To do so, use the *Group by: Expiration Date* option in the Centralized Certificates viewer, as Figure 3 shows.

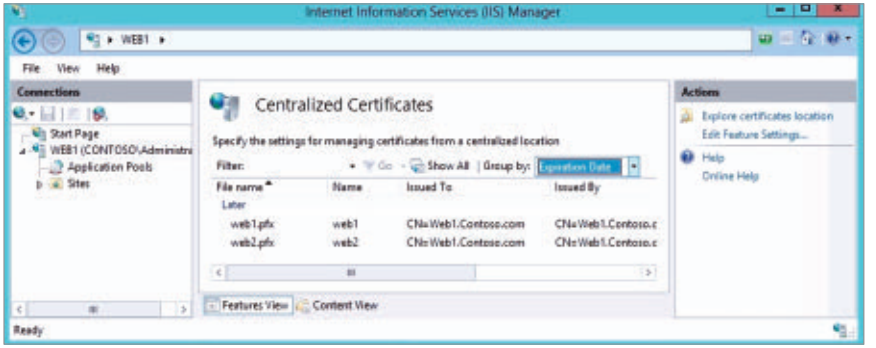


Figure 3
Grouping Certificates by Expiration Date in the IIS Centralized Certificates Viewer

To point a given website to the central SSL certificate store, you must select the new Use Centralized Certificate Store option in the configuration screen for creating a new website or the Site Bindings dialog box, as Figure 4 shows.

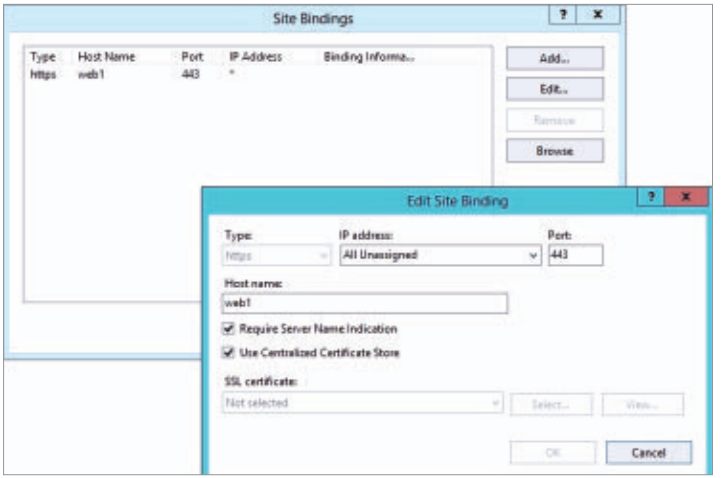


Figure 4
Using the Site Bindings Dialog Box to Point a Given Website to the Central SSL Certificate Store

Note that there's no need to select a specific certificate to be used. IIS leverages the site name that was entered in the configuration screen ("web1" in this example) to automatically select the corresponding SSL certificate in the central SSL certificate store.

—Jan De Clercq

Instant Doc ID 144887

Q: Can I run Windows RT within a Hyper-V virtual machine?

A: No, because a Hyper-V virtual machine (VM) can't run Windows RT. There are two reasons why:

- Windows RT isn't available for download—it comes preinstalled on Windows RT–based devices from OEMs.
- Windows RT is an OS for ARM processors—but Hyper-V supports x86/amd64 virtual processors, not ones based on ARM.

Even if Windows RT was downloadable, it couldn't run on the x86/amd64 processor. Therefore, it couldn't run in a VM on Hyper-V.

—John Savill

InstantDoc ID144932

Q: With a Windows 8 picture password, can you enforce complexity requirements?

A: Windows 8 lets you use a picture password consisting of three gestures that can be a point, line, or circle. It's not possible to enforce a certain level of complexity such as requiring a certain number of circles or to require more than three gestures.

—John Savill

InstantDoc ID144929



Windows Server 2012 Deployment

Learn the steps to deploy the top 5 roles for the OS

Although Windows Server 2012 has been out for quite some time now, few organizations have deployed it in their production environments. This isn't necessarily a reflection on Server 2012, which in my opinion is by far the best server OS that Microsoft has released (surpassing even Windows Server 2008 R2). Rather, it's an artifact of the way that organizations deploy server OSs. The lag between the release and general adoption of a server OS can stretch to years. This lag is likely to be even more pronounced with Server 2012, given that existing products such as Microsoft Exchange Server 2010 and SharePoint Server 2010 aren't supported on the OS. Some organizations will wait until they're ready to transition to Exchange Server 2013 and SharePoint Server 2013 before adopting Server 2012.

For those who are just beginning to consider deployment, this article details the steps to deploy Server 2012 in five common scenarios: as an Active Directory (AD) domain controller (DC), as a file server, and as the host OS for SQL Server 2012, Exchange 2013, and SharePoint 2013.



Orin Thomas

is a contributing editor for *Windows IT Pro* and a Windows Security MVP. He has authored or coauthored more than a dozen books for Microsoft Press.

Email

Blog

Side-by-Side Features

With Server 2008 R2, you didn't need to re-use the installation media after you installed the product. The installation process copied to a folder on the local hard disk all the required files for adding features. If you wanted to add a new role (e.g., AD, Background Intelligent Transfer Service—BITS), all you needed to do was run the wizard and you were on your way.

This isn't the case with Server 2012. To reduce the size of the Server 2012 installation footprint, Microsoft hasn't included all roles and features in the files that are copied when the OS is installed. Therefore, some features require access to the installation media when you try to install them by using the *Add Roles and Features* Wizard. One feature in particular that trips up many administrators when managing Server 2012 is the installation of .NET Framework 3.5 features.

When you attempt to install these features, you'll be prompted to enter an alternate source path, as Figure 1 shows. If the installation media is present, the alternate source path is the \sources\sxs folder. If the computer is connected to the Internet, then Server 2012 downloads the required files directly from Microsoft. You can also specify

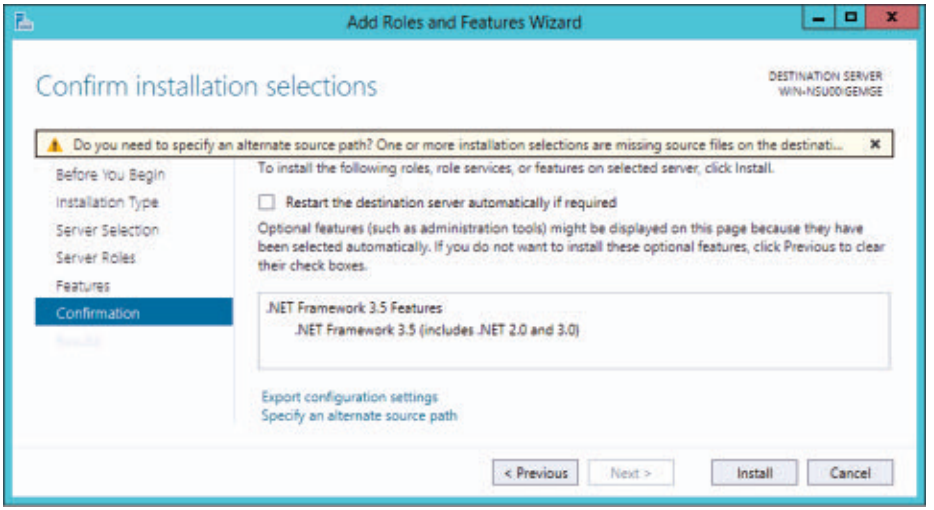


Figure 1
Prompt to Enter an Alternate Source Path

a network location, so creating a share and putting the sxs folder on that share ensures that you won't be scratching around for the installation media when you need it.

With Server 2012, you can install roles and features by using the *Add Roles and Features* Wizard or the Install-WindowsFeature Windows PowerShell cmdlet. If you use the cmdlet to install .NET Framework 3.5, you'll need to specify the source location in the command. This location can be the \sources\sxs folder of the installation media, an accessible install.wim file, or a parallel installation of Server 2012.

For example, if the installation media is located on volume E, you can install .NET Framework 3.5 features by running the following PowerShell command:

```
Install-WindowsFeature NET-Framework-Core –Source E:\Sources\SxS
```

.NET Framework 3.5 tends to trip up people because many products that run on Windows Server need it as a prerequisite. Unless your Server 2012 installation is connected to the Internet, you'll need to remember to have the installation media handy.

File servers running Windows Server 2012 have much better throughput than those running earlier versions of the Windows Server OS.

Active Directory Domain Controller

In previous versions of Windows Server, you promoted a computer to DC by running the dcpromo.exe utility. With Server 2012, the process is a little different. Many separate steps, such as having to run adprep.exe to prepare the forest and domain separately, are handled automatically when introducing a DC. There are numerous improvements in AD, including better support for virtualized DCs, DC cloning, and group managed service accounts. In Active Directory Administrative Center, you'll now find tools that vastly simplify the process of deploying fine-grained password policies and an intuitive interface for using Active Directory Recycle Bin. To learn more about the improvements in AD, see the Microsoft article "What's New in Active Directory Domain Services (AD DS)."

Before you deploy the DC role on a computer, you should do the following:

- Configure the computer with a static IPv4 address. Although you can configure a DC with an IP address that's assigned through a DHCP reservation, the setup wizard will recommend that you configure a static IPv4 address on the DC.
- Name the computer. When you install Server 2012, the computer is assigned a random name. Provide a meaningful name that describes the computer's role and location. For example, you might name the first DC in the city of Melbourne Melbourne-DC-1.
- Decide whether the DC will also function as a DNS server and as a Global Catalog (GC) server. Most administrators deploy the DNS role with DCs. You can also choose to configure the DC as a GC server or enable universal group membership caching.
- Decide on the Directory Services Restore Mode (DSRM) password. You need a password to perform directory restore mode operations. It's a good idea to have a uniform password across all DCs in your organization, rather than separate passwords for each DC. Uniform passwords ensure that restore operations can run more smoothly than they might if each DC has its own DSRM password.

To configure Server 2012 as a DC, perform these steps:

1. In the Server Manager console, click the Manage menu, and then click *Add Roles and Features*.
2. On the *Select installation* type page, choose *Role-based or feature-based installation*, as shown in Figure 2.
3. From the pool of servers, choose the server on which you want to install AD. Server 2012 allows you to manage multiple servers simultaneously, so you can use this wizard to deploy roles such as an AD DC to a local or remote server.
4. On the *Select server roles* page, choose Active Directory Domain Services. When you do this, you'll be prompted to install the

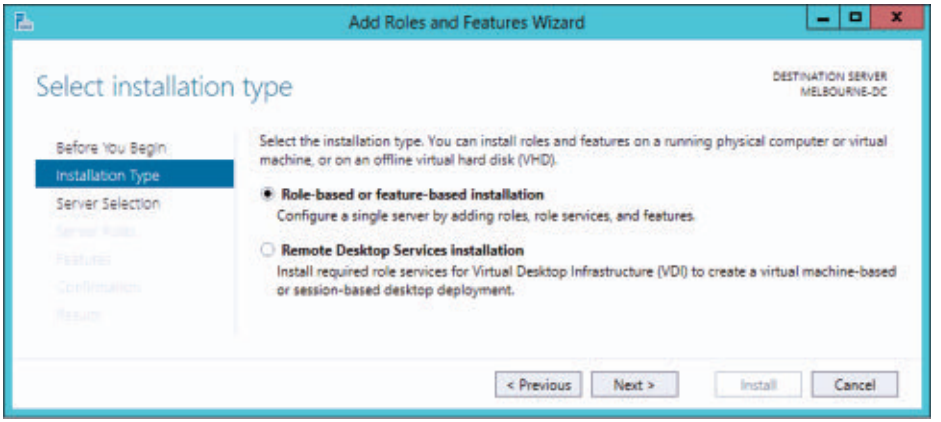


Figure 2
Server Installation Type Page

associated Remote Server Administration Tools if they haven't already been installed locally.

5. Click Next until you reach the page on which you can click Install. Click Install and the AD Directory Services binaries will be installed. Click Close to dismiss the *Add Roles and Features* Wizard.
6. On the *All Servers Task Details and Notifications* page, click *Promote this server to domain controller*.

Performing all these steps installs the AD components but doesn't actually promote the computer to DC. To do that, you'll need to perform these steps:

1. In Server Manager, click the AD DS workspace, and then click *Configuration required for Active Directory Domain Services*.
2. In the *All Servers Task Details and Notifications* dialog box, which Figure 3 shows, click *Promote this server to a domain controller*.
3. On the Deployment Configuration page, you'll be asked whether to add a DC to an existing domain, add a new domain to an existing forest, or add a new forest.
4. On the Domain Controller Options page, which Figure 4 shows, choose the domain and forest functional level. Also

Figure 3
All Servers Task Details and Notifications Page

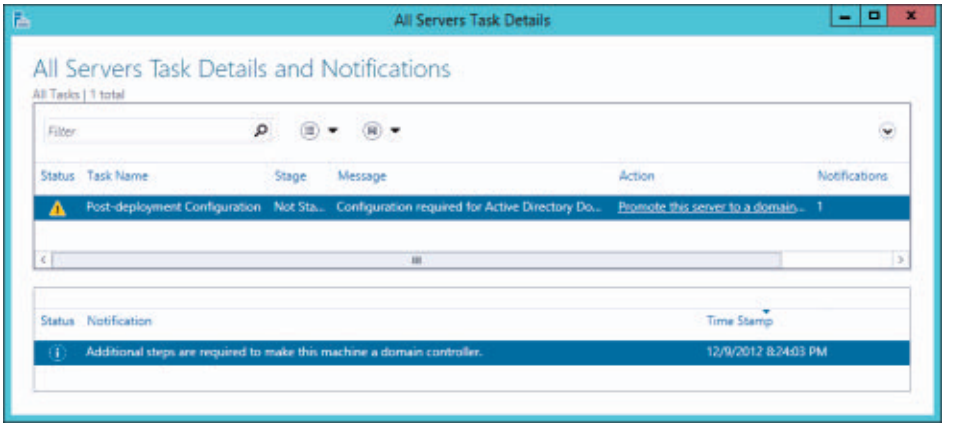
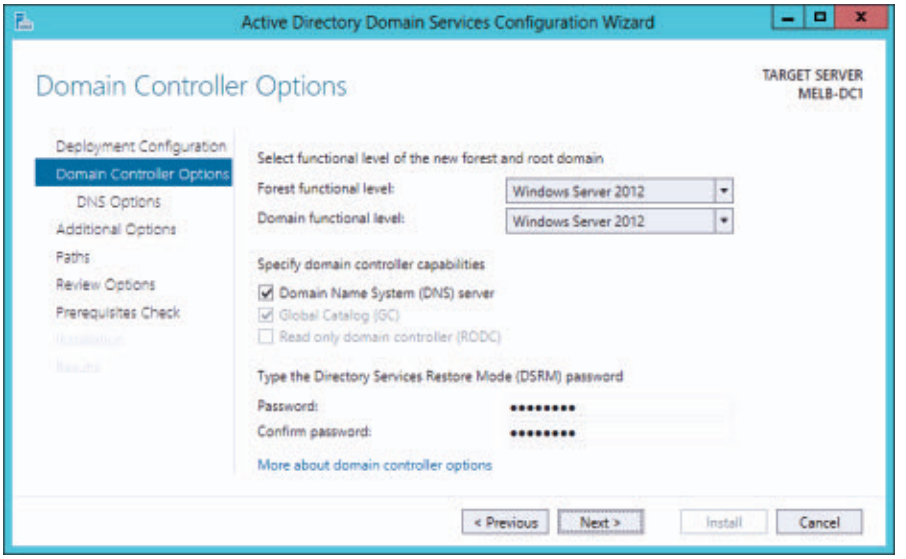


Figure 4
Domain Controller Options Page



choose whether you want the DC to function as a DNS server or GC server (the first DC in an organization must always be a GC server). Specify the DSRM password.

5. If you've chosen to deploy a DC, you'll be given the option of creating a DNS delegation.
6. If you're creating a new forest or a new domain, you'll be provided with an automatically generated NetBIOS name for the domain. This name can be modified if necessary.

7. On the Paths page, which Figure 5 shows, you can specify the database, log files, and SYSVOL folder to be used on the DC. In most cases, using the defaults is appropriate.

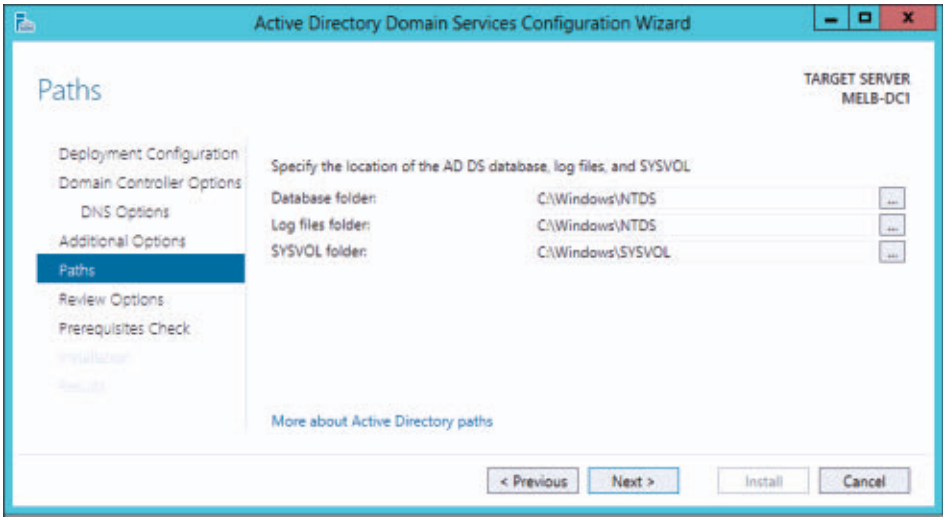


Figure 5
Paths Page

8. After you review your options, you can view a script that performs the installation. Figure 6 shows the use of the Install-ADDSForest PowerShell cmdlet to deploy and configure the DC role.

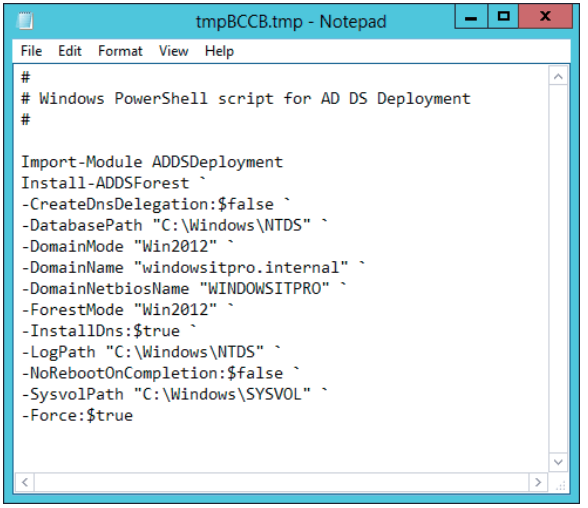


Figure 6
Install-ADDSForest PowerShell Cmdlet

9. After you've reviewed the selected installation options, a prerequisite check is performed. Assuming that the check is successful, you can install the DC role. The server will reboot to complete the promotion.

File Server

The file server role is the most commonly deployed role for computers running Server 2012. Almost every organization with Windows client OSs has at least one server functioning as a file server.

With Server 2012, Microsoft put a lot of work into improving the Server Message Block (SMB) protocol. File servers running Server 2012 have much better throughput than those running earlier versions of the Windows Server OS. File servers running Server 2012 can handle more clients than file servers running Server 2008 R2 and are much less likely to choke under heavy load. (You can find out more about the improvements in SMB 3.0 in the Microsoft article "Server Message Block Overview.")

In addition to the improvements to the SMB protocol, Server 2012 also supports storage spaces, a technology that allows you to create flexible and fault-tolerant virtual drives using multiple disks. Storage spaces are built into the OS, so you don't need to add any roles or features to use them. You can find out more about Storage Spaces in the Microsoft article "Storage Spaces Overview."

Deploying the File Server Role

The default installation of Server 2012 includes the file server role, so you can start sharing files immediately after completing installation. However, most organizations have more complicated needs, in which case you'll want to deploy more than one file server. The following role services can be deployed to computers running the full version or Server Core installation of Server 2012:

- File Server—Provides basic access to shared folders. This role is installed by default on a computer running Server 2012.
- BranchCache for Network Files—Allows the server to support BranchCache functionality, allowing files served to be stored on BranchCache clients across the WAN.
- Data Deduplication—Reduces disk utilization by storing only a single copy of data on a volume.

- DFS Namespaces—Allows you to create DFS namespaces.
- DFS Replication—Provides synchronization of files across branch offices.
- File Server Resource Manager—Allows you to create file screens, manage folder-level quotas, create file classifications, and generate storage reports.
- File Server VSS Agent Service—Allows applications that store data on the file server to create Volume Shadow Copy Service (VSS) snapshots.
- iSCSI Target Server—When installed, allows Server 2012 to function as an iSCSI target.
- iSCSI Target Storage Provider (VDS and VSS)—When installed, applications connected to an iSCSI target on the local server can create VSS snapshots.
- Server for NFS—Allows Server 2012 to function as an NFS server. NFS is primarily used by UNIX and Linux clients.
- Storage Services—Provides storage-management functionality.

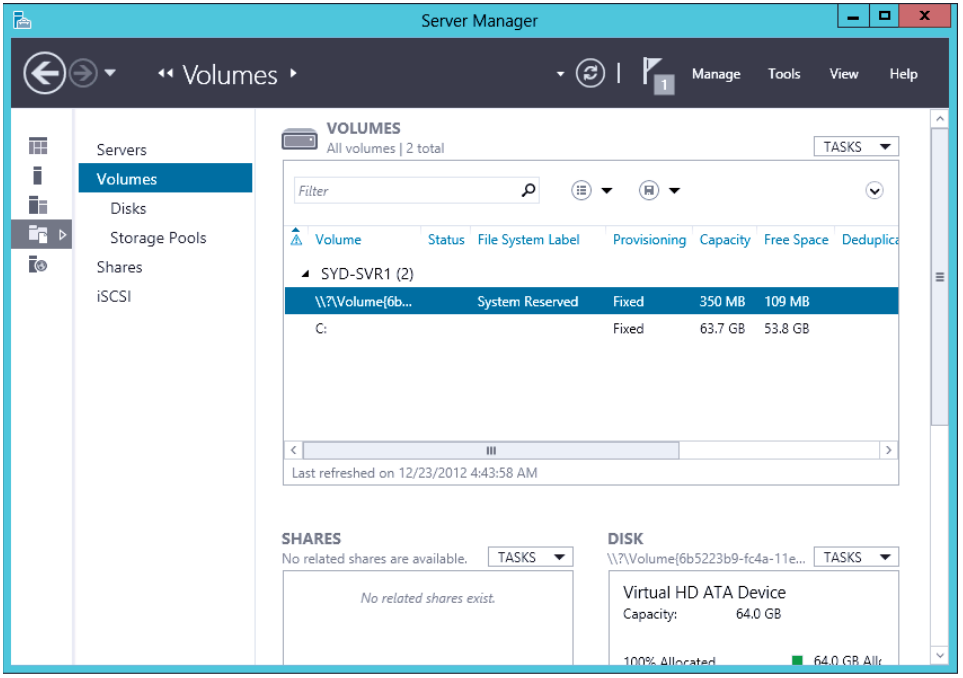
You can implement data deduplication only on the volumes that do not host the OS.

Managing the File Server

A big improvement in Server 2012 is the centralized nature of file and storage server management. In Server 2008 R2, you needed to use disparate consoles to manage file server–related tasks. For example, you used separate consoles to manage volumes, shares, iSCSI targets, file screens, and quotas. In Server 2012, these have all been co-located in the *File and Storage Services* section of the Server Manager console, as Figure 7 shows.

Choose the item that you want to work with—such as volumes, disks, shares, or iSCSI—from the list of objects in the left pane. You can then manage the details of those objects in the right pane. Remember Server 2012's multi-server management paradigm; you can use this

Figure 7
File and Storage Services



console to manage *File and Storage Services* on multiple servers, not just on the server where you've signed on. Being able to view the status of file shares and volumes across the organization from one console is far more efficient than the process used in Server 2008 R2 and earlier.

To create a new shared folder, perform the following steps:

1. In Server Manager, click *File and Storage Services*.
2. In *File and Storage Services,* click Shares.
3. Next to Shares, click Tasks, and then click New Share.
4. In the New Share Wizard, which Figure 8 shows, choose between file share profiles.

For most uses, the SMB Share - Quick option is appropriate. When you choose this option, specify the share location, name, permissions, and whether you want to enable features such as caching, access-based enumeration, BranchCache, and encrypted data access. Choosing the SMB Share - Quick option doesn't restrict you

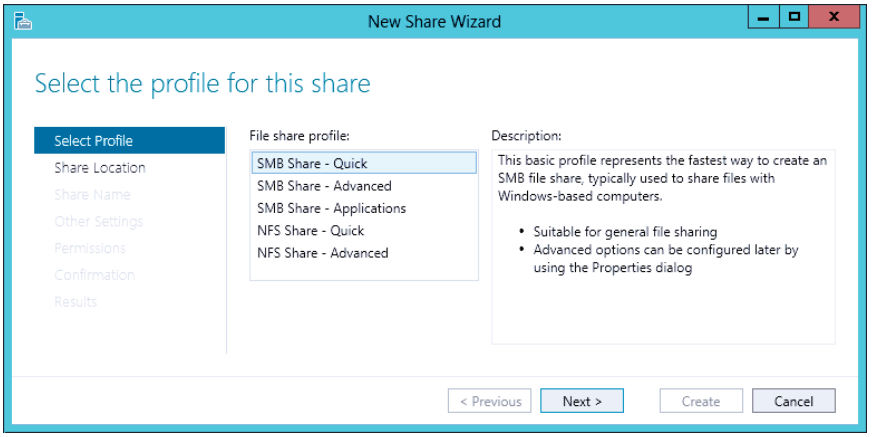


Figure 8
New Share Wizard

from later configuring advanced options, such as quotas and file screens. (Use the NFS options only if you're providing shared files to UNIX or Linux clients.)

SQL Server 2012

SQL Server is a prerequisite of many other Microsoft products, including the Microsoft System Center suite and SharePoint Server 2013. You can install SQL Server 2012 with Service Pack 1 (SP1) on computers running both the standard GUI and Server Core versions of Server 2012. (SQL Server is different than products such as SharePoint and Exchange, in that previous versions of SQL Server are supported on Server 2012. You can see the list of SQL Server editions and versions that Server 2012 supports by navigating to the Microsoft article "Using SQL Server in Windows 8 and Windows Server 2012 Environments." This article concentrates on SQL Server 2012 because you're more likely to deploy the most recent version of SQL Server on the most recent version of the Windows Server OS.)

SQL Server 2012 has the following requirements:

- .NET Framework 3.5 SP1 and .NET Framework 4.0
- PowerShell 2.0 or later (included by default with Server 2012)
- Microsoft IIS (required if you're installing SQL Server Reporting Services—SSRS)

SQL Server 2012 comes with a prerequisite checker that allows you to identify any missing components before they block you from installing the product. SQL Server 2012 supports the use of group managed service accounts and virtual accounts, defaulting to virtual accounts when installed on Server 2012. (You can view the SQL Server 2012 software and hardware requirements in the Microsoft article "Hardware and Software Requirements for Installing SQL Server 2012.")

Installing SQL Server in a default configuration, in which you install only the database engine and the default management tools, involves performing these steps:

1. On the splash screen, select *New SQL Server stand-alone installation,* or add features to an existing installation on the Installation tab.
2. The Setup Support Rules check will ensure that the basic requirements for installation have been met. Another check later in the process looks for feature-specific requirements. During this process, updated installation files can automatically be downloaded from the Microsoft website. The setup files are installed, allowing the next steps in the installation process to continue.
3. During the next stage in the installation process, enter the product key and agree to the license terms.
4. On the Setup Role page, choose whether to install specific features, SQL Server PowerPivot for SharePoint, or all features with defaults. In most cases, such as when SQL Server is supporting another product such as System Center 2012 Configuration Manager or Operations Manager, you need to install only a few features. As with any product, you should install only the features that you know you need, rather than the ones that you think you might need.
5. On the Feature Selection page, which Figure 9 shows, select the features that you want to install. (Figure 9 shows Database Engine services being installed. The management tools are also being installed, although that isn't visible in the figure.)

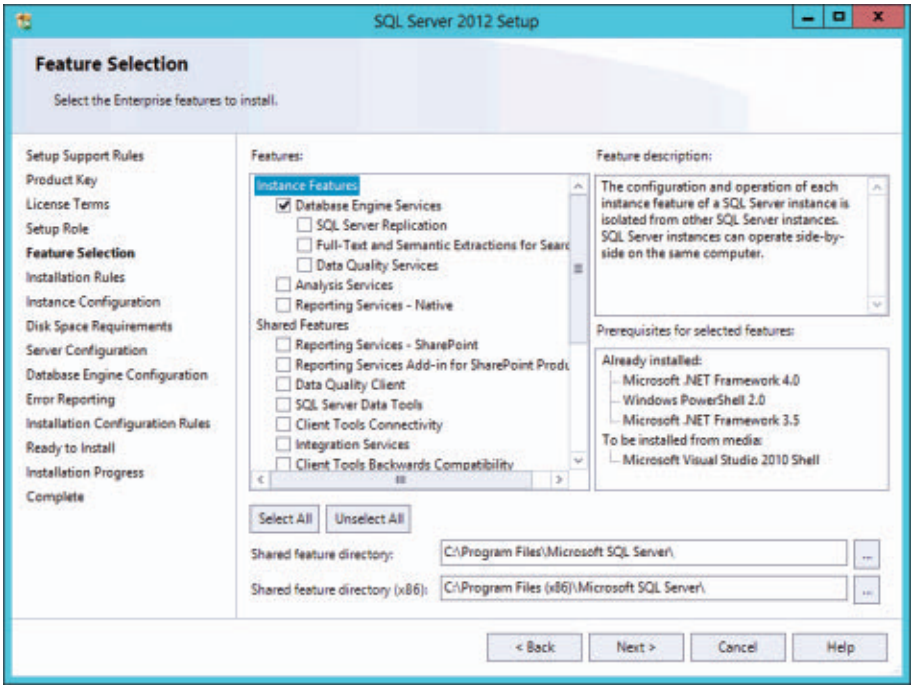
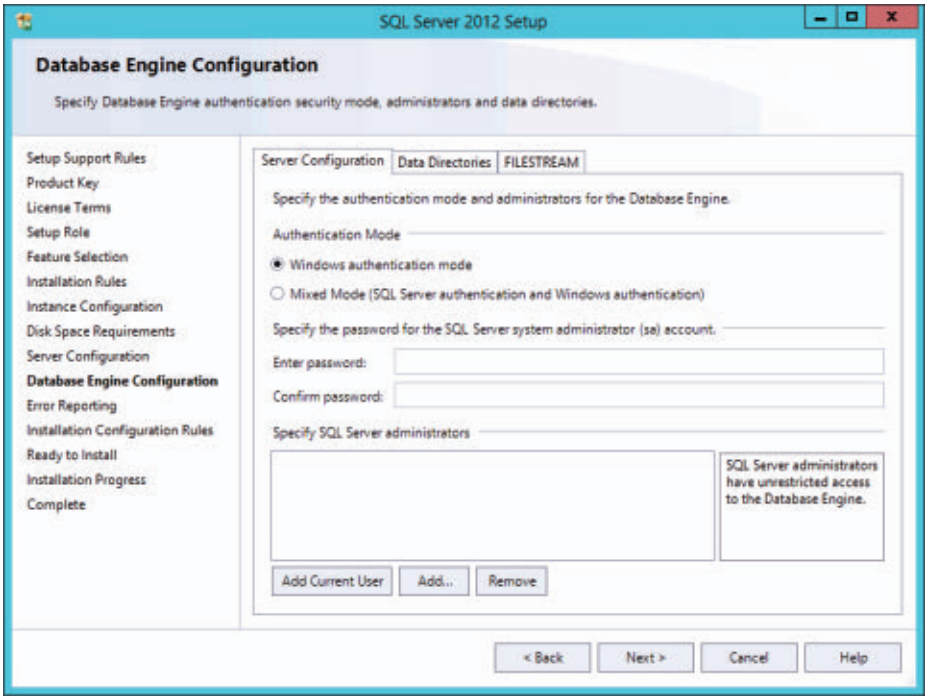


Figure 9
Installation of Database Engine Services

6. SQL Server performs another check to determine whether the desired configuration can be installed or whether there are blocking issues.
7. On the Instance Configuration page, choose whether to install SQL Server as a default or a named instance. If other instances are already installed on the server, they'll be listed in this dialog box.
8. SQL Server setup will then recommend that you use a default set of virtual service accounts. You can specify custom service accounts at this point, although the benefit of using virtual service accounts is that the OS manages the account's password, ensuring that it's changed on a regular basis. You can also choose which collation the SQL Server instance will use. If you're installing a SQL Server instance to support a specific product, you should determine whether the product requires a specific collation.

9. On the Database Engine Configuration page, which Figure 10 shows, choose which users will have SQL Server administrator privileges. On this page, you also choose the authentication mode. Most modern applications use Windows authentication, but some older applications might require mixed mode, which allows you to use SQL Server authentication.

Figure 10
Database Engine Configuration Page



10. SQL Server is now ready to install. Although installing SQL Server doesn't require that you reboot the server, it's a good idea to do so. Then use SQL Server Management Studio to connect to the instance and verify that everything works.

Exchange Server 2013

You can install Exchange 2013 on computers running Server 2008 R2 or Server 2012. To prepare AD for Exchange 2013 deployment, you need to have .NET Framework 4.5 and Windows Management Framework 3.0

installed. (Both are included with the default installation of Server 2012 and don't need to be installed separately.) You also need to have deployed the AD Directory Services–related Remote Server Administration Tools. You can install these tools by using the *Add Roles and Features* Wizard or by executing the following PowerShell command:

```
Install-WindowsFeature RSAT-ADDS
```

Exchange 2013 also requires that the schema master, GC server, and at least one DC in each site run Windows Server 2003 with SP2 or later. The forest functional level must be Windows Server 2003 or later. It's fairly safe to assume that if you're thinking of deploying Exchange 2013 on Server 2012, your organization's infrastructure meets these requirements.

If you're going to install both the Mailbox server and Client Access server roles on a computer running Server 2012, you can install them all by running the PowerShell command that Listing 1 shows. You'll need to restart the server after the command executes. You'll then need to install the following software, which you can download from the Microsoft website, in this order:

1. Microsoft Unified Communications Managed API 4.0, Core Runtime (64-bit)
2. Microsoft Office 2010 Filter Pack (64-bit)
3. Microsoft Office 2010 Filter Pack SP1 (64-bit)

Listing 1: PowerShell Command to Install Mailbox Server and Client Access Server Roles

```
Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-
Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface,
Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-
Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors,
Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-
Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service,
Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-
Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation
```

After you've installed these components, you can install Exchange 2013 by performing the following steps:

1. Run Setup from the installation media. You'll be prompted to check for updated installation files, to agree to the license agreement, and to decide whether to provide feedback to Microsoft.
2. On the Server Role Selection page, which Figure 11 shows, you can choose whether to install the Mailbox server role or the Client Access server role. You can also configure the Exchange 2013 installation routine to automatically install any roles and features that are required to support Exchange, although it's better to do this prior to starting the installation routine.

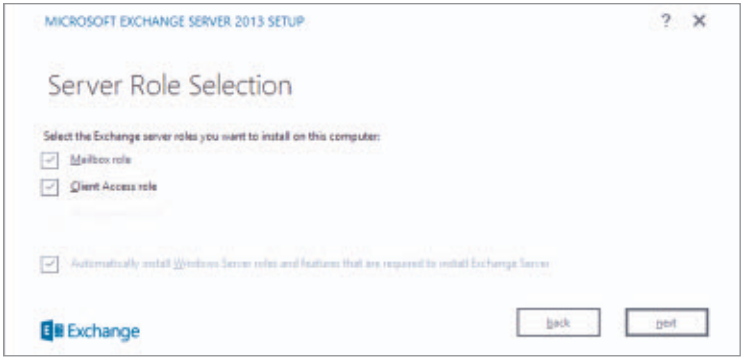


Figure 11 Server Role Selection Page

3. You'll be prompted to specify the location of the Exchange installation files and to choose a name for your Exchange organization. You can also choose to apply AD split permissions, if you want to separate the administration of AD and Exchange.
4. Choose whether to disable native malware scanning. (The only reason that you'd do so is if you're using a third-party product for malware protection on your Exchange server.)
5. The installation routine performs a prerequisite check and analysis. After these checks are passed, you can install Exchange 2013. As long as you have the AD Directory Services Remote Server Administration Tools installed, any preparation of AD prior to deployment will occur automatically.

6. After installation completes, you can verify the success of the installation by using a web browser to navigate to the Exchange Administrative Center. A link to this page is provided on the final page of the installation wizard.

As you use a web browser to manage Exchange 2013, you might find it useful to pin the Exchange Administrative Center website address to the taskbar of the computer on which you have installed Exchange 2013. (You can find the Exchange 2013 prerequisites listed in the Microsoft article "Exchange 2013 System Requirements.")

SharePoint 2013

There are many ways to install SharePoint 2013. The simplest is to install a single server using a built-in database.

The SharePoint Products Preparation Tool installs the following roles, features, and additional software:

- Web Server (IIS) role
- Application Server role
- .NET Framework 4.5
- SQL Server 2008 R2 SP1 Native Client
- Microsoft WCF Data Services 5.0
- Microsoft Information Protection and Control Client (IPC)
- Microsoft Sync Framework Runtime v1.0 SP1 (x64)
- Windows Management Framework 3.0, which includes PowerShell 3.0
- Windows Identity Foundation (WIF) 1.0 and Microsoft Identity Extensions (previously WIF 1.1)
- Windows Server AppFabric
- Cumulative Update Package 1 for Microsoft AppFabric 1.1 for Windows Server

You can run this tool by running prerequisiteinstaller.exe from the root folder of the SharePoint 2013 installation media. Unless you have

copies of all the required local files in addition to the roles and features, such as the SQL Server 2008 R2 SP1 Native Client, you need to have an Internet connection to successfully run this tool. Running the preparation tool necessitates one or more reboots. The preparation tool will continue to run after reboot, until all prerequisites have been installed or enabled.

After all the prerequisite components have been installed, you can install SharePoint Server 2013 by performing the following steps:

1. Provide your SharePoint 2013 product key and agree to the license terms.
2. Choose either a complete or standalone installation. The latter installs a local instance of SQL Server 2008 R2 Express with SP1 and isn't recommended for production environments. If you choose a complete installation, you need to have administrative access to an instance of SQL Server 2008 R2 SP1 or later. The installation of SQL Server 2012 described earlier in this article can function in this role.
3. After installation is complete, you must run the SharePoint Products Configuration Wizard. This wizard is launched by default when you complete the installation wizard.
4. When running the configuration wizard and setting up a new SharePoint 2013 deployment, choose to create a new server farm. Specify the location of the database name and the account of a user that has administrative permissions on the instance, as Figure 12 shows.
5. Configure a farm passphrase. You'll use this passphrase whenever you want to join new servers to the SharePoint 2013 farm.
6. On the Configure SharePoint Central Administration Web Application page, choose a port number for the web application or allow one to be selected at random. You can also choose between NTLM and Kerberos authentication, with NTLM being the default value.

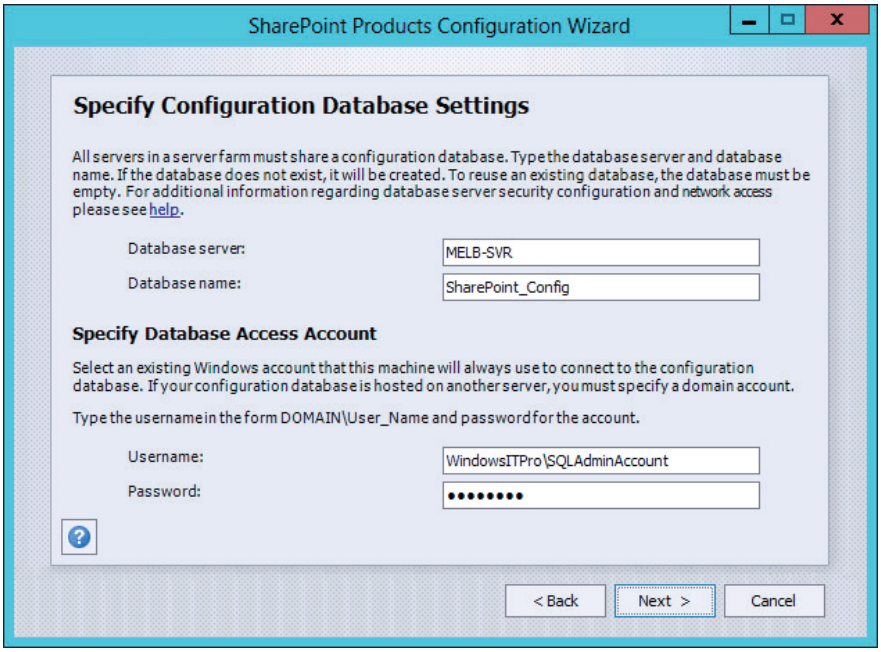


Figure 12
Creating a New Server Farm

When configuration is complete, you can connect to the SharePoint Central Administration website to complete the configuration of SharePoint 2013. (The Microsoft article "Hardware and Software Requirements for SharePoint 2013" shows the requirements for a single SharePoint server with a built-in database.)

Straightforward Deployment

This article has described how to deploy common Server 2012 roles. Although I've shown you how to deploy products such as Exchange 2013, SharePoint 2013, and SQL Server 2012, I haven't covered the post-installation configuration steps that you need to take to customize each of these products before deploying them to a production environment. Deployment of these roles and products on Server 2012 is straightforward. The only thing that you need to do is review the system requirements pages on TechNet and ensure that the appropriate roles and features are installed or available before you begin deployment. ■

InstantDoc ID 145025

Windows Server 2012

Improvements in storage, virtualization, and management are worth a look

Windows Server 2012, arguably the most significant server release Microsoft has ever offered, became available for evaluation and purchase to customers around the world on September 4, 2012. Server 2012 offers a simplified licensing model that includes all features of the OS in all editions of Server. You'll find improved management capabilities in Server Manager and PowerShell. Storage improvements are numerous, and Hyper-V enhancements include scalability, live migration upgrades, and storage live migration capabilities. *Windows IT Pro* brings you ongoing coverage of Server 2012, with in-depth treatment of significant features, breaking news, and analysis. Visit our Windows Server 2012 page for the latest news and technical features. ■

InstantDoc ID 143935

Top 10 Windows Server 2012 FAQs

1. PowerShell Module Automatic Load in Windows 8 and Server 2012
2. Downgrade Windows Server 2012 Datacenter to Server 2012 Standard?
3. Use Server 2012 Data Deduplication Even if My SAN is Already Doing It?
4. System Center Configuration Manager for Windows 8 and Windows 2012
5. Find Microsoft Limits for Hyper-V
6. How do I remotely view a Remote Desktop session in Windows Server 2012?
7. What features does NTFS support that ReFS does not support?
8. How many network adapters can be combined in a single Windows Server 2012 native NIC team in a virtual machine?
9. I'm using Windows PowerShell to create a new Windows Server 2012 native NIC team, so why isn't the -Confirm flag working to suppress the configuration prompt?
10. How many network adapters can be combined in a single Windows Server 2012 and nativeNIC team on a physical host?

Windows Server 2012 Articles

- Configuring Hyper-V Replica in Windows Server 2012
- Hyper-V Replica for Disaster Recovery
- Troubleshooting Windows Server 2012 Virtualized Domain Controller Cloning
- Managing Hyper-V with PowerShell
- Microsoft's Cloud OS: A Vision of Infrastructure's Future
- Navigating Storage Spaces and Pools
- Integrating vSphere and Hyper-V
- Introducing Windows Server 2012
- New Features in Windows Server 2012 Server Manager
- Windows Server 2012 Essentials: Access the Server Remotely
- Windows Server 2012 Sprints Through the Finish Line
- Getting Around in Windows Server 2012, Part 2: Server Manager
- Windows Server 2012 Essentials: Domain vs. Workgroup
- Get Ready for Windows Server 2012 Hyper-V
- Cloning Virtual Domain Controllers in Windows Server 2012
- Windows Server 2012: Foundation vs. Essentials
- Video: Getting Around in Windows Server 2012 Server Manager
- Windows Server 2012 Essentials: Connect Client PCs without Using a Domain
- Windows Server 2012 and SQL Server 2012: Better Together
- New Ways to Enable High Availability for File Shares
- Microsoft Releases Windows Server 2012 to Manufacturing
- Top 10 Windows Server 2012 Storage Enhancements

www.windowsitpro.com/windows-server-2012

Windows Server 2012 Hyper-V Security Features

Network Virtualization and other changes boost flexibility and manageability



Jan De Clercq

is a member of HP's Technology Consulting IT Assurance Portfolio team. He focuses on cloud security, identity and access management, architecture for Microsoft-rooted IT infrastructures, and security of Microsoft products. He's the co-author of *Microsoft Windows Security Fundamentals* (Digital Press).

Email

Windows Server 2012 and Hyper-V are fundamental building blocks of Microsoft's private cloud strategy. The most recent Microsoft server OS comes with Microsoft Hyper-V 3.0 hypervisor, which features many changes. Hyper-V 3.0 might become the first Microsoft virtualization platform to truly challenge VMware vSphere.

Among the Hyper-V changes are several new security features. Network Virtualization is Microsoft's first step in the Software-Defined Networking (SDN) space. In SDN, the control of network traffic is managed by software that runs outside the physical network hardware, allowing more flexible network management and configuration. From a security point of view, SDN and Network Virtualization enable organizations and cloud providers to better isolate virtual machines (VMs) on the network level.

There are also many smaller—though no less important—security-related changes in Hyper-V 3.0. Good examples are the new extensible virtual network switch, the new Hyper-V Administrators group, and enhanced Windows BitLocker Drive Encryption support.

Defining Network Virtualization

With Network Virtualization, Microsoft extends its VM isolation capabilities from the host to the network layer. Isolation is crucial in multi-tenant cloud solutions, in which the applications and services of different organizations or organizational departments are hosted

on the same physical server and network infrastructure. For example, a cloud provider that hosts services for both Apple and Samsung certainly wouldn't want Apple to sneak into Samsung's VMs or network, or vice versa.

Similar to the way that server virtualization allows you to set up multiple isolated VMs on a single host, Hyper-V 3.0 Network Virtualization allows you to run multiple isolated virtual networks on the same physical network. Network Virtualization leverages a software-based abstraction layer that sits on top of the physical network and is based on the concept of virtual subnets. A virtual subnet represents a broadcast boundary that ensures that only VMs on the same virtual subnet can communicate with one another. As such, virtual subnets allow administrators to set up different isolated broadcast domains between VMs.

Although Hyper-V has supported the use of virtual LANs (VLANs) for the creation of isolated virtual networks since Windows Server 2008, VLANs have limited scalability and flexibility. VLANs can support only a limited number of isolated tenant networks. This limit exists primarily because switches typically don't support more than 1,000 VLAN IDs out of the theoretical limit of 4,096. According to Microsoft, Network Virtualization can support more than 16 million virtual networks.

Furthermore, VLANs lack flexibility. They are poorly suited for dynamic cloud environments, in which tenant VMs regularly join and leave the data center and migrate across physical servers for load-balancing or capacity-management purposes. VLAN management is complex and requires reconfigurations on the switch level when a VM is moved to another host. Server 2012 also adds support for private VLANs (PVLANs), through an extension on the level of the Hyper-V virtual switch. Although PVLANs can increase the level of isolation between VMs, they don't counter the problem of complex VLAN management across virtual and physical networking devices. This problem can be addressed only through the use of Network Virtualization.

Under the Network Virtualization Hood

With Network Virtualization, each VM is assigned two IP addresses. One IP address is visible to the VM and is relevant only in the context of a given tenant virtual or software-defined network. This address is called the Customer Address (CA). The second IP address is relevant only in the context of the physical network. This address is called the Provider Address (PA). The decoupling of CA and PA brings several benefits.

First, customers easily move VMs between data centers. Thanks to the new abstraction layer, you can move a VM to the data center of another cloud service provider, without reconfiguring the VM's IP and network configuration and without changing all the IP address–based policies in the organization. You also don't need to worry anymore about the IP configuration of other tenants' VMs that are hosted in the same data center. When Network Virtualization is enabled, VMs with identical IP addresses can coexist on the same Hyper-V host and even on the same network, without IP address conflicts.

Network Virtualization also allows the live migration of VMs between physical servers on different subnets, without service interruption. If a VM has two IP addresses, then the PA can be changed without affecting the CA. A user or application that talks to the VM by using the CA will not experience interruptions and will be unaware that the VM has physically moved to a different subnet.

Besides CAs and PAs, Network Virtualization uses a third important component: the Virtual Subnet ID (VSID). Each Network Virtualization virtual subnet is uniquely identified using a VSID. VSIDs allow Hyper-V hosts to tag traffic from different virtual subnets and to differentiate the traffic of VMs that have the same CA. The Network Virtualization software logic encapsulates the VSID, CA, and PA into each network packet.

To allow specific tenant networks to span multiple virtual subnets (and thus IP subnets), VSIDs can also be grouped into a single customer network that is then uniquely identified by using a Routing Domain ID

(RDID). In these situations, Network Virtualization's isolation will be enforced on the level of the defined customer networks. This is another difference between Network Virtualization virtual networks and traditional VLANs: VLANs can be linked only to a single IP subnet.

Network Virtualization requires only a Server 2012 Hyper-V host. With Network Virtualization the guest OS in the VM is totally unaware that its IP address is being virtualized. From the VM's perspective, all communication occurs using its CA. This also means that a VM that is part of a Network Virtualization–based network can run any OS: not only Windows 8 and Server 2012, but also older Windows versions and other OSs.

Figure 1 illustrates how Network Virtualization is implemented under the hood. Basically, Network Virtualization is implemented as a new network driver (called ms_netwnv) that can be bound to physical network adapter cards on each Server 2012 physical server and virtual server. The new Hyper-V virtual switch, which I'll come back to later in this article, calls on this network driver to encapsulate and de-encapsulate Network Virtualization network packets.

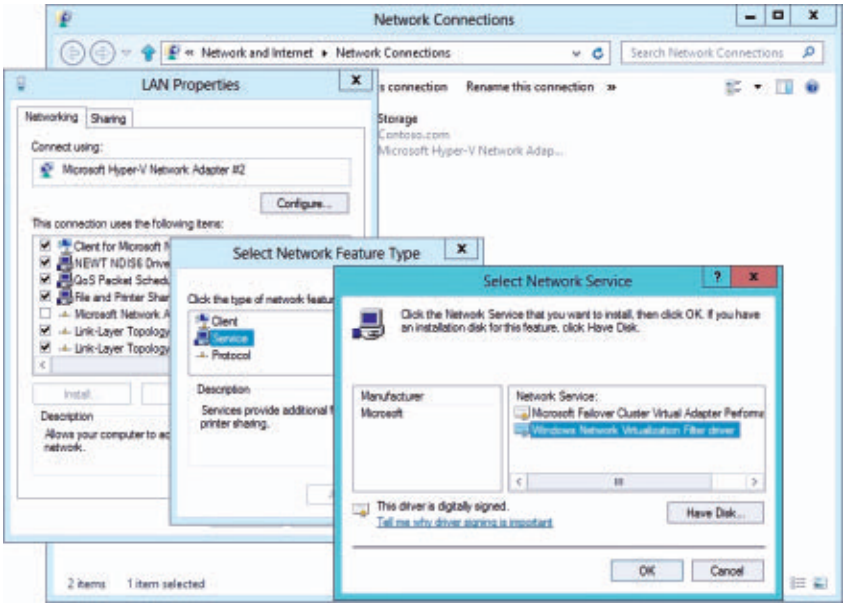


Figure 1 Implementing Network Virtualization as a Network Filter Driver

Transporting and Routing Network Virtualization

To transport and route IP packets with virtualized CAs across the physical network, Network Virtualization can use two mechanisms. The first mechanism is based on the Generic Routing Encapsulation (GRE) tunneling protocol that's defined in Request for Comments (RFCs) 2784 and 2890. In this context, GRE is used to encapsulate the network packets that are generated by a VM (with a CA) into packets that are generated by the host (with a PA). Together with other cloud industry players (e.g., HP, Intel, Emulex, Dell), Microsoft has submitted a draft to the Internet Engineering Task Force (IETF) to make the Network Virtualization variation of GRE (called NVGRE) a standard.

The second mechanism, IP address rewrite, can be compared with Network Address Translation (NAT). This mechanism rewrites packets with virtualized CAs to packets with PAs, which can be routed across the physical network.

At the time of writing, IP address rewrite is better suited for VMs with high throughput requirements (i.e., 10Gbps) because it can leverage network adapter card hardware-level offload mechanisms such as large send offload (LSO) and virtual machine queue (VMQ). A big disadvantage of IP address rewrite is that it requires one unique PA for each VM CA. Otherwise, differentiating and routing the network packets from and to VMs that belong to different tenants with overlapping IP addresses would not be possible.

Because GRE requires only one PA per host, Microsoft recommends using NVGRE over IP address rewrite for Network Virtualization. NVGRE can be implemented without making changes to the physical network switch architecture. NVGRE tunnels are terminated on the Hyper-V hosts and process all the encapsulating and de-encapsulating of GRE network traffic.

One disadvantage of GRE is that it can't leverage the network adapter card hardware-level offload mechanisms. Therefore, if you plan to use NVGRE to virtualize high network throughputs, I advise you to wait for the availability of network adapter cards that support

NVGRE offloading. Microsoft expects vendors to release such cards for Server 2012 later this year. When using GRE, also watch out for existing firewalls that might have default GRE blocking rules. Always make sure that such firewalls are reconfigured to allow GRE (IP Protocol 47) tunnel traffic.

Implementing Network Virtualization

Hyper-V 3.0 might become the first Microsoft virtualization platform to truly challenge VMware vSphere.

The process for implementing and configuring Hyper-V 3.0 Network Virtualization is different than that for setting up VLANs in Hyper-V. You can configure VLANs from the Hyper-V Manager in the VM network adapter settings. Network Virtualization configuration isn't part of a VM's configuration and can't be done from the Hyper-V Manager. This is because Network Virtualization is based on specific policies that are enforced on the virtual-switch level of a Hyper-V host.

To define Network Virtualization policies locally on the host, you must use Windows PowerShell scripts. To define the policies centrally, you can use the Microsoft System Center Virtual Machine Manager (VMM) Service Pack 1 (SP1) GUI. VMM is Microsoft's unified management solution for VMs. In larger Network Virtualization environments, I strongly recommend that you leverage VMM. VMM can run the correct PowerShell cmdlets on your behalf and enforce the Network Virtualization policies on the Hyper-V host through local System Center host agents. An important limitation at the time of this writing is that the VMM GUI can be used only to define IP address rewrite policies. To define NVGRE policies, you must use PowerShell scripts. To get you started configuring Network Virtualization by using PowerShell, Microsoft provides a sample PowerShell script in its Simple Hyper-V Network Virtualization Demo.

When you want to use NVGRE, you should also plan for Network Virtualization gateway functionality. A Network Virtualization gateway is needed to enable a VM on a virtual network to communicate outside of that virtual network. A Network Virtualization gateway understands and knows the Network Virtualization address-mapping

policies. The gateway can translate network packets that are encapsulated with NVGRE to non-encapsulated packets, and vice versa.

Network Virtualization gateways come in different form factors. They can be built on a VPN gateway that creates a VPN connection to link two virtualized networks across a physical network. For this purpose, you can use a Server 2012 server that's running RRAS. Network Virtualization gateway functionality can also be provided by a dedicated networking device (e.g., a switch, a network appliance) that acts as a routing gateway for Network Virtualization. At the time of this writing, Network Virtualization gateway appliances are provided or being planned by F5 Networks and nAppliance Networks. To configure the Network Virtualization gateways, you can use PowerShell. To get started, see the sample script in the Microsoft article "Simple Hyper-V Network Virtualization Script with Gateway."

Luckily, VMM SP1 also includes extensions to centrally and automatically manage Network Virtualization Gateway policies. When a VM is created or updated, VMM can automatically update the routing topology of each Network Virtualization gateway device. For more information about Network Virtualization gateways, see the Microsoft article "Hyper-V Network Virtualization Gateway Architectural Guide."

For much more information about Network Virtualization in general, see the Microsoft article "Microsoft Windows Server 2012 Hyper-V Network Virtualization Survival Guide." A nice summary of the steps that you must follow to set up Network Virtualization is also available in the Microsoft TechNet blog post "Step-by-Step: Hyper-V Network Virtualization."

Extensible Virtual Switch

In Hyper-V 3.0, Microsoft also made significant changes to its virtual switch architecture—now referred to as the extensible switch. This Layer 2 virtual network switch can be configured on each Hyper-V host and is at the intersection of network traffic between VMs, between

VMs and the Hyper-V host, and with external machines. The extensible switch is the Hyper-V component that enforces Network Virtualization policies and includes other interesting, security-related features.

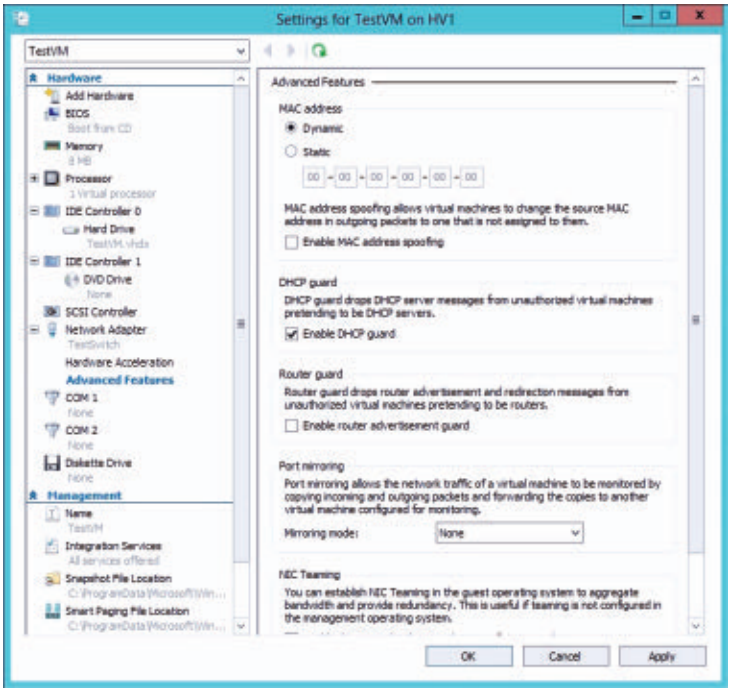
Microsoft partners can build extensible switch extensions that use the Windows Filtering Platform (WFP) or Windows network device interface specification (NDIS) filters to monitor or modify network packets, authorize connections, or filter traffic. Thanks to this new architecture, the extensible switch can enforce security and isolation policies when connecting VMs to the network. A virtual switch is the ideal place to scan the inter-VM traffic on a host for malware. Classic malware and intrusion prevention solutions typically cannot scan this traffic and can examine only physical host-to-host traffic. A few Microsoft partners that have already jumped on the extensible-switch bandwagon are sFlow, which provides a monitoring extension; 5nine, which provides a virtual firewall extension; and NEC, which provides an OpenFlow-based monitoring extension. OpenFlow is an important open-source protocol for SDN.

The new extensible switch also supports the definition of PVLANs. Administrators can create PVLANs by assigning a VM to a primary VLAN and then to one or more secondary VLANs. Using these PVLANs, administrators can ensure that VMs either can communicate only with VMs with the same VLAN ID or IDs or can communicate with any other VM with the same primary VLAN ID, regardless of secondary VLAN ID. As I pointed out earlier, PVLANs don't counter the complexity of VLAN management across virtual and physical networking devices. These problems can be addressed only through the use of Network Virtualization.

Another powerful extensible switch feature is the ACL-based isolation policies that can be defined and enforced on the extensible switch virtual ports. These policies are basically lists of Allow and Deny rules that ensure that VMs are isolated and can't communicate with other VMs based on their IP or MAC addresses. These extensible switch isolation policies can also be defined from VMM.

Finally, the extensible switch supports new security features such as DHCP Guard, IPsec Task Offload, and protection against Address Resolution Protocol (ARP) poisoning. DHCP Guard can be used to prevent VMs from acting as a DHCP server. DHCP Guard works by dropping any packets that a VM attempts to send that would indicate that it's a DHCP server. DHCP Guard is a property that can be configured for each VM network adapter. You can do so from the Hyper-V Manager, in the Advanced Features section of the network adapter settings in the VM properties, as Figure 2 shows. I recommend that you enable this setting during the creation of your VM golden image.

Figure 2
Enabling DHCP Guard



IPsec Task Offload allows Hyper-V to offload IPsec-related processing to a network adapter. This is possible only when the network adapter supports the feature. IPsec Task Offload can reduce the Hyper-V host-processor performance hit that's associated with the use of IPsec encryption algorithms. You can also enable this setting

from Hyper-V Manager: Use the Hardware Acceleration section of the network adapter settings in the VM properties, as Figure 3 shows.

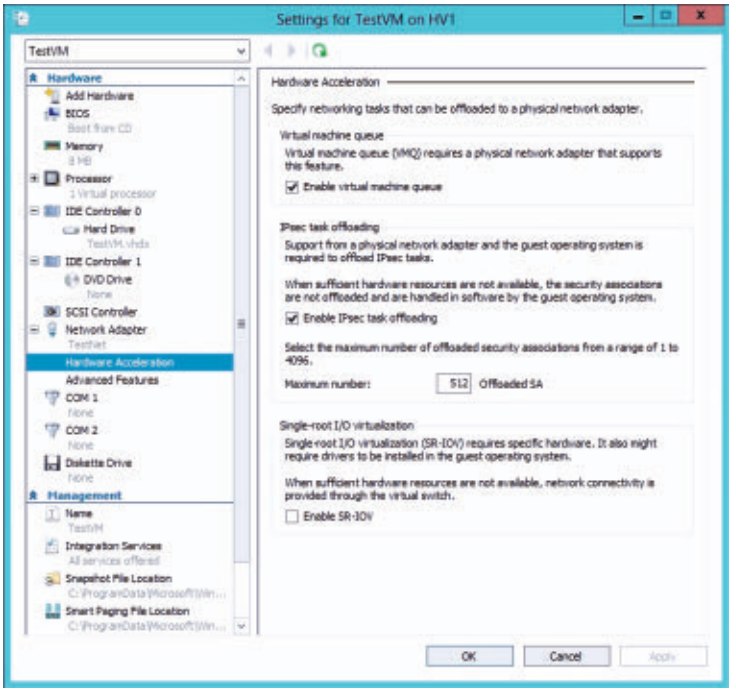


Figure 3
Enabling IPsec Task Offload

The extensible switch includes protection against ARP poisoning to ensure that malicious VMs can't launch an ARP poisoning–based man-in-the-middle attack. In such an attack, a malicious machine uses fake ARP messages to associate malicious MAC addresses with IP addresses that it doesn't own. This can make unsuspecting machines send messages to the malicious machine instead of other intended destination machines. To enable ARP poisoning protection, you must leave the *Enable MAC address spoofing* check box in its default clear state.

To make it easier to configure the extensible switch and its extensions, Microsoft provides PowerShell cmdlets. You can use these to create automated scripts for extensible switch configuration, monitoring, or troubleshooting.

Simplified Delegation, BitLocker Extension

Hyper-V 3.0 supports simplified administrative delegation through the introduction of the Hyper-V Administrators local security group. Members of this new group have complete access to all Hyper-V features. Administrators should use this group to control access to Hyper-V, instead of adding users to the local Administrators group. The new group is also a partial replacement for the Windows Authorization Manager (AzMan), which was previously the only available solution for setting up administrative delegation in Hyper-V. Administrators can continue to use AzMan for delegation scenarios that need more granularity and that go beyond assigning the complete Hyper-V Administrator role.

Finally I want to point out that in Server 2012 you can also take advantage of the new BitLocker volume-level encryption features to protect the confidentiality and integrity of VM images that might be stored in less physically secure locations. Server 2012 BitLocker has been extended to support the encryption of OS and data volumes on Windows failover cluster disks, including cluster shared volumes. See "BitLocker Changes in Windows 8" for more information.

Important vSphere Security Differentiators

The new security features are important differentiators when positioning Hyper-V against its close competitor, VMware vSphere. A good example is the new Hyper-V extensible switch. VMware also offers a virtual network switch, but it's available only in the high-end Enterprise Plus edition of vSphere, which comes at an extra cost. The vSphere switch isn't open or extensible, nor does it come with some of the advanced security features (e.g., DHCP Guard, virtual port ACLs) of the Hyper-V switch. Such features can be added to vSphere only through the purchase of additional software, such as the App component of the VMware vCloud Networking and Security (vCNS) suite.

Similar observations can be made for the Hyper-V Network Virtualization feature. To obtain similar functionality in a vSphere environment,

customers must call on the vCNS suite, which supports a technology known as VXLAN. VXLAN also require the vSphere Distributed Switch (VDS), which comes only with the high-end edition of vSphere. (VMware is expected to ramp up in the SDN space soon, through its recent acquisition of Nicira.)

Powerful Flexibility

In summary, Hyper-V 3.0 comes with powerful new security features that also benefit the overall flexibility and manageability of Hyper-V–based multi-tenant clouds. Now is the time to learn more about the new Hyper-V. Also make sure that you familiarize yourself with the new capabilities in VVM SP1, which is an indispensable tool for managing larger Hyper-V deployments. ■

InstantDoc ID 144923

Windows 8

The new client OS represents a radical departure from previous Windows versions

Windows 8, Microsoft's latest client OS, features a new UI designed to be tablet touch-friendly, and became available to customers via software upgrades or with new PC purchases on October 26, 2012. Windows 8 represents a radical departure from previous Windows versions and is arguably the most dramatic upgrade Microsoft has yet developed.

The system is essentially a brand-new mobile platform that has been melded onto the traditional Windows desktop, giving users what Microsoft calls a "no compromises" experience that blends the best of mobile with the best of Windows. *Windows IT Pro* brings you ongoing coverage of Windows 8, with in-depth treatment of significant features, breaking news, and analysis. Visit our Windows 8 page for the latest news and technical features. ■

InstantDoc ID 144099

Windows 8 In-Depth

- Windows 8 Myths
- The Windows 8 Battle Moves from Software to Devices
- Windows 8 for the Win: Touch + Mobility + Cloud
- 20 Windows 8 Devices that Wowed the Crowds at CES
- Video: Windows 8 Keyboard and Mouse Survival Guide
- Windows 8 Client Virtualization
- Welcome to Windows 8
- Upgrade from Windows 8 Enterprise Eval? Nope
- Windows 8 Review, Part 1: The Desktop
- Windows 8 Review, Part 2: You Got Your Metro in My Windows
- Windows 8 Upgrade Offer for PC Buyers Goes Live
- Start: The Windows 8 Era Begins

Windows 8 Features

- Windows 8 Feature Focus: Windows Store
- Windows 8 Feature Focus: Settings Sync
- Windows 8 Feature Focus: File Explorer
- Windows 8 Feature Focus: Live Tiles
- Windows 8 Feature Focus: From Pre-Release to RTM
- Windows 8 Feature Focus: Charms
- Windows 8 Feature Focus: Start Screen
- Windows 8 Feature Focus: Lock Screen
- Windows 8 Feature Focus: Back Tip
- Windows 8 Feature Focus: Tiles
- Windows 8 Feature Focus: Contracts

Windows 8 Tips

- Windows 8 Tip: Buy the Electronic Upgrade Now, Install It Later
- Windows 8 Tip: Shut Down Metro-Style Apps
- Windows 8 Tip: Upgrade to Windows 8 Now
- Windows 8 Tip: Use Windows 7 System Image Backup
- Windows 8 Tip: Complete Windows 8 with Windows Essentials 2012
- Windows 8 Tip: Use Trackpad Multi-touch Gestures
- Windows 8 Tip: Pin Favorite Apps in Start Search
- Windows 8 Tip: Picking a Backup Strategy
- Windows 8 Tip: Upgrade from Windows 7
- Windows 8 Tip: Upgrade from Windows XP
- Windows 8 Tip: Upgrade from Windows Vista
- Windows 8 Tip: Upgrade from the Release Preview

www.windowsitpro.com/windows-8

Office 365: Time to Make the Switch?

Top 10 pros and cons



Tony Redmond

is a senior contributing editor for *Windows IT Pro* and the author of *Microsoft Exchange Server 2010 Inside Out* (Microsoft Press).

Email

Twitter

Blog

Microsoft Office 365, launched formally in June 2011, is a strategic project for Microsoft. The signs are that Microsoft has been successful in convincing many companies of the solution's advantages.

As a subscriber, I'm happy with Office 365, despite some hiccups that have marred its reliability record. Still, I'm amused by the hype that surrounds many Office 365 discussions. In this article, I bring together 10 points that supporters often stress when making a case for Office 365—and I seek to balance the debate with 10 points of caution. You undoubtedly have your own view, but each of these arguments has sense to it—so read both lists with an open mind!

10 Advantages of Office 365

Given the enormous investment that Microsoft has made in data centers, software engineering, operations, and staff to build, deploy, and manage Office 365, it's not surprising that the service is an easy sell. This list describes the top 10 advantages that companies can gain if they move to Office 365.

1 ***Predictable ongoing costs.*** Knowing what your costs will be on a month-to-month basis is the number-one advantage put forward by Office 365 supporters. Microsoft offers a range of Office 365 plans, each represented by different functionality. You can host email only (the Exchange Online plan). Or you can go higher, through plans that are designed for professionals and small businesses (the P plans), up to those intended for use by larger enterprises (the E plans). In March 2012, Microsoft reduced the prices for some plans to reflect

competitive needs and to take account of customer feedback. In particular, the four E plans received reductions of 18 to 20 percent. Even though Microsoft hasn't reduced the monthly cost of the Office 365 Plan P subscription from $6, it's still a relative bargain for the functionality. This is especially true if you already have a copy of Office 2013, 2010, or 2007 that you can use to connect to Office 365. (The array of available plans can be confusing at first, so it pays to consult someone who is familiar with Office 365 to determine the best plan for your business.)

Whichever plan you choose, the key factor in realizing benefits from Office 365 is to ensure that current IT spending is reallocated to productive purposes rather than to areas that don't contribute to the bottom line. For example, opting for a cloud service releases funds that would otherwise be spent on servers, storage, and hardware maintenance. These funds could be used to develop new software applications that improve and streamline business processes. Or they could be used to fund investment in some other area of technology, such as equipping the sales force with new mobile devices.

2 ***Service expandability.*** It's great to be able to add or remove subscriptions at will and pay only for what you use on a monthly basis. Although you might end up paying for unused subscriptions (in the same way that on-premises licenses are often unused after purchase), the nature of the monthly payment draws natural attention to the number of subscriptions and makes it easier for small-to-midsized businesses (SMBs) to track costs.

Microsoft still has some work to do. Making better usage reporting available through the administration portal would be appreciated. It would also be useful if Microsoft would remove the block that stops small companies that use Plan P subscriptions from easily moving to Plan E. This block just doesn't make sense: You never know when growth will come to a company, and it's unnatural for a cloud service to build in artificial blocks that inhibit expandability.

3 ***No more software maintenance.*** Eliminating software maintenance is a big deal, especially for anyone running Microsoft Exchange Server 2007 or Exchange Server 2003 and wondering about the cost and effort required to migrate to Exchange Server 2013. Add the necessity of keeping track as Microsoft releases service packs, roll-up updates, and future versions—and the need to determine that nothing in them will cause problems within your environment. (This is an issue that we've seen with roll-up updates for Exchange 2010 during 2011 and 2012.)

4 ***Reliability.*** The reliability factor of Office 365 isn't so much a 99.9 percent service level agreement (SLA); Microsoft hasn't actually achieved this level of performance for any reasonable length of time. (Four notable outages have occurred while Office 365 has been in full production, but it's fair to say that these outages did not affect all users of the service.) At this point, Microsoft needs to keep plugging away to meet its own SLA goals and then match the performance that Google has achieved for its cloud services.

I prefer to focus on the fact that Office 365 delivers better availability to users than most SMB IT organizations can provide. Let's face it: There's no comparison between the availability that can be provided by a server in an office (the anecdotal computer under the desk) and the power of a modern data center. That being said, even the oldest computer in a local office delivers better availability if you can't connect to a remote data center because of some Internet problem or insufficient bandwidth.

5 ***Client choice.*** Fat and feature-rich clients such as Microsoft Outlook often get the most attention when the discussion turns to clients. But it's much more interesting to consider the recent work that Microsoft has done in the area of web and mobile clients. In the case of Exchange, the Outlook Web App (OWA) client runs on Microsoft Internet Explorer (IE), Google Chrome, Mozilla Firefox, Apple Safari, and other browsers and does a pretty good job across multiple platforms. But if you're using a mobile client, you're more likely to use one that takes advantage of the many Microsoft ActiveSync licensing deals that the company has

made with major mobile device vendors over the past few years. From iOS to Android to Windows Phone to Windows RT, ActiveSync makes a connection possible.

6 ***Access.*** SMBs (or sometimes even large companies) can find it difficult to build and operate an infrastructure that supports secure remote access for users. You immediately get this access on a worldwide basis when you subscribe to Office 365—and you can use all the clients that we've just discussed. After you experience anywhere access, you'll never want to go back to traveling to the office to read email or access a Microsoft SharePoint site. It's just so much more productive to be able to work anytime, anywhere. Although Office 365 supports dual-factor authentication methods that might be insufficient for some companies that have specific requirements, I suspect that many of these access issues will be solved as time goes by.

7 ***An array of on-premises and hybrid options.*** Cloud services are absolutely the right choice for some companies. Others will never want to go near the cloud for reasons that make sense in context. And a large group in the middle can make use of cloud services for some purposes but want to keep a portion of their capability on-premises. The choice of available deployment options for Exchange, SharePoint, and Lync—as well as the work that Microsoft has done to enable essential features such as single-sign on (SSO) and the ability to move data freely between platforms—delivers huge flexibility to companies as they consider their options. More work to continually improve and make hybrid configurations easier to create and maintain will likely happen over the next few years. For example, the creation of the Hybrid Configuration Wizard in Exchange 2010 Service Pack 2 (SP2) is a great example of how to automate many manual steps.

Another point to consider is how on-premises deployments should benefit from the improvements in system automation and other aspects of systems administration that Microsoft simply must deliver

to drive efficiencies in its data centers. I see a lot of this focus in Windows Server 2012. It will be interesting to see this story evolve over the next several years.

8 ***Additional value pools to exploit.*** Many companies will see sufficient value in moving to Office 365 for email alone. They can replace their current (and potentially old) Exchange servers with Exchange Online, a discussion that's bound to take place as companies that run Exchange 2003 today consider their future options. The nice thing about Office 365 is that email is a great start, but it's only that—a start. Enormous value can be extracted by enabling online collaboration with Lync Online or document management with SharePoint. And Exchange administrators who worry about losing their jobs as work transitions to the cloud can deliver new value working with SharePoint and Lync.

9 ***Security.*** Microsoft has exerted enormous effort to ensure that its data centers meet every conceivable security and audit requirement that pertains under multiple jurisdictions. Some issues exist (e.g., the potential requirement for Microsoft to make data available under the US Patriot Act, making its data centers less attractive for non-American companies). Still, anyone who has had the opportunity to visit a Microsoft data center can attest to the physical security that exists to prevent unauthorized access. The same dedication exists at the software level. Microsoft understands that a breach of security that exposes Office 365 customer data to unauthorized access would have a huge and continuing impact on its business. Given the experience and expertise available to Microsoft in both its engineering groups and data-center operations, I suspect that the company will do a better job of keeping customer data secure than even those customers' IT departments can do.

10 ***Ease of transition.*** Office 365 supports a variety of transition options to meet the requirements of differently sized companies. Some will be able to move to Office 365 with a certain amount of planning and a single "big bang" operation over a weekend. Others will use

a phased approach and move tens, hundreds, or even thousands of users weekly until the whole company has been transitioned. And others will maintain a hybrid configuration on an ongoing basis.

The important thing is that there are sufficient high-quality tools available to migrate from older versions of Microsoft technology as well as from other platforms (e.g., Novell GroupWise, Lotus Notes, and IMAP or POP3 email systems). Some of these tools must be bought from third parties; others are free from Microsoft. All take a certain amount of planning. The old truism that each hour's preparation pays big benefits is as valid here as in any software project.

This list makes Office 365 look good. In fact, for some it's a pretty compelling offering. But there are downsides to consuming a cloud service. After all, you don't expect to exert much control over the Apple iTunes service or to tell Amazon how to run its Elastic Compute Cloud (EC2). We must therefore consider the downside before plunging into the cloud.

10 Potential Problems with Office 365

Much value can be extracted from Office 365. And it's natural for small companies that aren't IT literate to dedicate resources doing what they do best rather than figuring out the complexities of deploying and managing software. It's easy to imagine that a large proportion of SMBs with IT based around Windows Small Business Server and the associated applications will move to Office 365 over the next few years (assuming that sufficient Internet connectivity is available). However, the decision to move platforms becomes more complex as the number of users grows.

The following list offers some points that might negatively influence the decision to move to Office 365. Like any technology debate, it's important to put the negative points in context and weigh them up against the advantages, to arrive at a balanced decision for your company.

1 ***Reliability.*** Yes, this item is also on the list of advantages. After all, Office 365 delivers a reliable and robust service—most of the time. However, several high-profile outages have taken some gloss from the service. The root causes appear to be operational lapses of the type that you would hope wouldn't occur. These outages might be indicative of growing pains that have been eliminated and will not recur. But the first goal for Office 365 is to first meet its own 99.9 percent SLA over an extended period, then to surpass the service performance delivered by its major rival. In the end, whether reliability comes in as a plus or a minus depends on your company.

2 ***Lack of flexibility.*** Office 365 is a bounded service. In other words, if what you want to do is already available, you'll be happy. But don't ask for additional features. The Office 365 team can't provide specific features for individual customers. Everyone gets to use the same service and access the same feature set. Microsoft will update Office 365 with bug fixes, service packs, new features, and new versions according to its own schedule. It's entirely possible that a desired feature *might* appear in one of these updates. If not, you'll need to wait.

Another potential issue relates to integration. You won't enjoy the flexibility you might expect in connecting applications to support business processes. For example, many companies integrate application provisioning (e.g., creating an Active Directory—AD—account, setting up an Exchange mailbox, and populating a SharePoint personal site) into the process of adding new employees. (Or conversely, they integrate the process of eliminating these items when employees leave.) By using Windows PowerShell, this approach might still be possible with Office 365, but it's definitely something you need to confirm first.

3 ***Support for older clients.*** Many companies still use Outlook 2003, a client that Office 365 doesn't support, at least not for Messaging API (MAPI) connections. The reason is simple: Office 365 doesn't support public folders, so it can't offer the free/busy and Offline Address Book (OAB) service to Outlook clients that depend on public folders. This isn't an issue if you have plans to deploy a more modern client

(Outlook 2010 or 2013 is recommended), but companies are often surprised when they discover that older clients can't be connected. (Note that Exchange 2013 doesn't support Outlook 2003 clients either, so you'll also face the question about what to do with these clients if you plan to stay on-premises.)

4 ***Migrations.*** Smiles break out on administrator faces whenever migrations are proposed. It's such a fun activity. Seriously though, migrations are usually costly, extended affairs with a high potential for error. Given sufficient preparation, small companies with a few hundred users can migrate to Office 365 over a weekend. Larger companies, especially those that want to keep some work on-premises, have a lot more work to do over a longer period. They might need to deploy additional hardware and software—for example, to support AD Federation Services (ADFS)—or use the services of external consultants who have experience linking to Office 365, especially when complex AD configurations are in use. All this results in additional cost that must be factored into the overall project.

5 ***Realistic cost assessment.*** Making the decision to pay $6/month for 10 users isn't going to break the bank and is usually a cost-effective move for a small company. The calculation isn't so straightforward as the number of users rises. Many IT administrators figure that they can provide a better service to their company for the same amount as Office 365 will charge, after everything is factored into the decision. Therefore, it's important to think past the simple, low-cost-per-month equation that marketing and sales teams push and look at the overall cost to deploy, manage, and maintain the systems that you need over a reasonable period (i.e., 3 or 4 years).

You might be able to save money by squeezing some additional time out of server hardware, not upgrading client software, or eliminating software licenses that you don't need. In this respect, you should focus on what people need to do their jobs rather than on headline features. For example, access to email on the road is now a business essential; a 25GB mailbox is a nice-to-have (it takes so long

for most people to accumulate that much email). On the credit side, you might be able to deliver a better and more flexible service than the "all-in-one" service from Office 365. A focus on adding value to the business by solving business problems rather than simply delivering technology is always appreciated and might tip the balance.

6 ***Inconsistency across Office 365 applications.*** Despite the existence of Microsoft Business Productivity Online Suite (BPOS), a previous iteration of online applications that proved to be as reliable as its name was unloved, much of the Office 365 infrastructure is very much in its first version. (Microsoft will upgrade the Exchange, Lync, and SharePoint applications in 2013.) The actual user clients, such as OWA, are well-developed and functional. However, the administrative interfaces were clearly developed by three engineering groups who obviously didn't spend much time talking to one another. Of course, Microsoft is in the middle of a transition from traditional server-management techniques to the kind of remote management that's envisaged in Server 2012, so it's probably understandable that the three Office 365 applications present different views of how to manage settings. More consistency is expected in the future.

7 ***The one-in-a-crowd support experience.*** Office 365 depends on email and phone support and encourages users to help themselves with online troubleshooting tools and forums. Although this approach is perfectly understandable in terms of reducing costs, DIY support might come as a culture shock for companies that have become accustomed to the more personal interaction that often occurs with a local Microsoft office. Even if your local Microsoft team remains engaged, it won't be able to assist when problems occur with Office 365. Support for Office 365 follows a factory model with extremely tight and well-defined processes that apply to everyone. Thus, instead of being an individual customer who receives individual support based on a support plan that was negotiated with the local Microsoft office, you become one in a million and receive exactly the same support—good or bad—as everyone else.

8 ***Public folders.*** As mentioned earlier, Office 365 doesn't support public folders. Microsoft has published a guide to migration from public folders, which essentially recommends that anyone using Exchange public folders today should move to other repositories, such as Exchange shared mailboxes or SharePoint Online. This approach is viable when public folders are used for simple storage or document management. Everything becomes much more complex when users depend on electronic forms or any other enhanced use of public folders. Unless the applications are no longer required or can be replaced with something like an intelligent Microsoft Excel worksheet, you might need to rewrite applications. That's usually an expensive and long process. Microsoft does plan to support "modern" public folders when Exchange 2013 is used by Office 365. However, the migration path is uncertain, untested, and unknown at this point.

9 ***Inflexible administration tools.*** Compared with on-premises deployment, the administrative tools that are available for Office 365 can be inflexible. Microsoft's response will probably be that the tools are designed to work within a well-defined structure and to serve the needs of service users. The point is that when you control your own administrative environment, you can make whichever changes make sense. For example, you can deploy a specific mobile-device monitoring tool to ensure that your ActiveSync-compliant devices are functioning properly. Or you can install programs to analyze Exchange message-tracking logs, to extract statistics about message volume, top senders, and so on. But when you opt for a cloud service, you must accept that the service is bounded and therefore can't be tailored to meet individual requirements; doing so would create a support nightmare. APIs such as Exchange Web Services do expose data that can be used. But there's a dearth of third-party products available that work against Office 365, compared with on-premises servers. The balance will likely shift eventually, but that hasn't happened yet.

10 ***No Plan B.*** Microsoft obviously offers a lot of support to companies that want to move to Office 365. But what's the situation if a company decides that the cloud doesn't work for it?

Those who run hybrid Exchange deployments can move mailboxes back to on-premises servers reasonably easily, gradually backing out of Office 365. After the last mailbox is moved, the federation trust can be broken to isolate the on-premises servers. To complete the move, any data that resides in SharePoint Online must be moved to on-premises servers; conferencing must be moved to on-premises Lync servers. This is all possible, but as far as I know, it hasn't been done to date. Things are a little more complex for companies that have gone through a big-bang migration. These companies have no link to on-premises servers and therefore must plan for a second big-bang migration to move *back* to their own computing resources. Mailboxes can be exported to personal folder stores (PSTs) and imported back onto on-premises servers; SharePoint documents can likewise be exported and imported; and Lync servers are set up to take over conferencing. Once again, these approaches are all possible but probably expensive in terms of planning and execution.

It's All Up to You

At the end of the day, the decision to stay with on-premises technology or to move to a cloud computing service is highly specific to the stresses and demands that exist within individual companies. The points that I've outlined here are rather broad and represent only a starting point for the debate. The decision will be easy for some and thorny for others. In either case, carry out the necessary due diligence before making your choice. ■

InstantDoc ID 142737

Comparing File Version Numbers in VBScript and PowerShell

These simple script functions make comparisons a snap

Systems administrators often need to know file-version information—for example, to determine whether a software patch has been applied. The information is metadata, embedded in a Windows executable (e.g., .exe, .dll) file as a set of dot-delimited numbers, such as 12.1.42.0. From left to right, these numbers indicate major version, minor version, build, and revision. Each number is a 16-bit, unsigned integer. The first two numbers (i.e., major and minor version) represent the most significant 32 bits of the version number. The last two numbers (i.e., build and revision) represent the least significant 32 bits of the version number.

In Windows Script Host (WSH) scripts, you can retrieve a file's version by using the FileSystemObject object's GetFileVersion method. For example, the code in Listing 1 is a short VBScript script that outputs the file version of Notepad.exe.

In Windows PowerShell, you can use the VersionInfo property of a file object, which returns a .NET FileVersionInfo object. This object

Listing 1: Retrieving a File's Version in VBScript

```
Dim FSO, FileName
Set FSO = CreateObject("Scripting.FileSystemObject")
FileName = "C:\Windows\system32\notepad.exe"
WScript.Echo FSO.GetFileVersion(FileName)
```



Bill Stewart

is a scripting guru who works for Indian Health Service in Albuquerque, New Mexico. He's a contributing editor for *Windows IT Pro* and a moderator for Microsoft's Scripting Guys forum. He offers free tools on his website.

Email

Website

has four properties—FileMajorPart, FileMinorPart, FileBuildPart, and FilePrivatePart—that correspond to the four parts of the version number. The code in Listing 2 shows a short PowerShell function that uses the -f operator to output the version of Notepad.exe. This listing also shows how you can use the FileSystemObject in PowerShell to get the same information.

Listing 2: Retrieving a File's Version in PowerShell

```
$fileName = "C:\Windows\system32\notepad.exe"

function get-fileversion {
  param([System.IO.FileInfo] $fileItem)
  $verInfo = $fileItem.VersionInfo
  "{0}.{1}.{2}.{3}" -f
    $verInfo.FileMajorPart,
    $verInfo.FileMinorPart,
    $verInfo.FileBuildPart,
    $verInfo.FilePrivatePart
}

# Outputs the file's version
get-fileversion $fileName

# You can also use the FileSystemObject object's GetFileVersion method.
$fso = new-object -comobject "Scripting.FileSystemObject"

# Same output as previous get-fileversion function.
$fso.GetFileVersion($fileName)
```

So far, so good. But retrieving file versions is one thing; how do we *compare* those version numbers? We've already seen that a file-version number is actually a 64-bit, unsigned integer. VBScript doesn't have a 64-bit unsigned integer type. PowerShell has the UInt64 type, but not all PowerShell operators work with this type. To solve these problems, I wrote some VBScript and PowerShell script functions

that take the pain out of comparing version numbers. Before presenting these functions, though, I need to give you a bit of background about how they work.

Step 1: Break Down the Bits

Retrieving file versions is one thing; how do we *compare* those version numbers?

We can't use 64-bit numbers directly in VBScript, and we can't use these numbers in PowerShell without some missing operator support. So we'll begin by breaking down the version number into a pair of 32-bit numbers. Because we can't easily compare two 64-bit values, we'll compare two pairs of 32-bit values instead.

First, you need to know how to convert a string *a.b*, where *a* is the most significant 16 bits and *b* is the least significant 16 bits, into one 32-bit value. We can't simply interpret the string as a floating-point number, or the comparison won't work properly. For example, as floating-point numbers, 5.20 is equal to 5.2. In that scenario, 5.15 is the greater number (because 15 is greater than 2). In a version-number situation, that's obviously not the case: 5.20 is greater than 5.15.

To correctly convert the string *a.b* into a single 32-bit number, we perform a left shift on the first number and then add the second number to it. To illustrate, let's use the programmer mode in the Windows 7 calculator.

Open the calculator, Select View, Programmer, and then select the Hex and Dword radio buttons along the left edge of the window. (The effects are easier to observe in hexadecimal than in decimal.) In this example, we'll create a 32-bit number that represents the version number 3.7. Follow these steps in the calculator:

1. Enter the number 3, for the major version.
2. Click the Lsh button, enter the value 10 (i.e., hexadecimal for 16), and press Enter. This action shifts the number 16 bits to the left.
3. Press +, then press 7, and then press Enter. This action adds the minor version.

The resulting value is hexadecimal 30007, as shown in Figure 1.

Thus, the formula for converting the string *a.b* to a single 32-bit value is as follows:

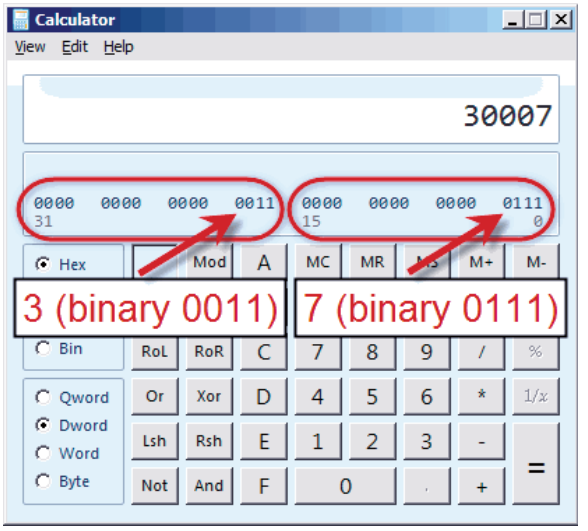


Figure 1
Sample Hexadecimal of a Converted String

$$(a \text{ Lsh } 16) + b$$

Because VBScript and PowerShell don't have an Lsh operator, we'll use the following equivalent formula instead:

$$(a * 216) + b$$

I previously mentioned that I decided to break the 64 bits of a version number into two 32-bit numbers. In the script code, I decided to return the two 32-bit numbers as a two-element array. For example, the version number 3.7.5.1 would be returned as an array containing the values 196615 (30007 hexadecimal for 3.7) and 327681 (50001 hexadecimal for 5.1).

Table 1: Comparing Version Numbers

Condition	Result
a.b < w.x	*a.b.c.d < w.x.y.z*
a.b = w.x and c.d < x.y	*a.b.c.d < w.x.y.z*
a.b = w.x and c.d = x.y	*a.b.c.d = w.x.y.z*
a.b = w.x and c.d > x.y	*a.b.c.d > w.x.y.z*
a.b > w.x	*a.b.c.d > w.x.y.z*

Step 2: Compare the Versions

So far, we've seen that we can represent a 64-bit value as a pair of 32-bit values. The question now is how do we compare those values? Given two version numbers *a.b.c.d* and *w.x.y.z*, Table 1 shows the possible comparison results.

Step 3: Writing the Code

Now that you understand the nature of file-version numbers and how to compare them, we're ready to take a look at the VBScript and PowerShell code that does the work. Listing 3 contains the VBScript functions, and Listing 4 contains the same functions written in PowerShell. These functions are described in Table 2.

Listing 3: VBScript Functions

```
' Bitwise left shift
Function Lsh(ByVal N, ByVal Bits)
  Lsh = N * (2 ^ Bits)
End Function

' Returns a version string "a.b.c.d" as a two-element numeric
' array. The first array element is the most significant 32 bits,
' and the second element is the least significant 32 bits.
Function GetVersionStringAsArray(ByVal Version)
  Dim VersionAll, VersionParts, N
  VersionAll = Array(0, 0, 0, 0)
  VersionParts = Split(Version, ".")
  For N = 0 To UBound(VersionParts)
    VersionAll(N) = CLng(VersionParts(N))
  Next

  Dim Hi, Lo
  Hi = Lsh(VersionAll(0), 16) + VersionAll(1)
  Lo = Lsh(VersionAll(2), 16) + VersionAll(3)

  GetVersionStringAsArray = Array(Hi, Lo)
End Function

' Compares two versions "a.b.c.d". If Version1 < Version2,
' returns -1. If Version1 = Version2, returns 0.
' If Version1 > Version2, returns 1.
Function CompareVersions(ByVal Version1, ByVal Version2)
```

Listing 3: *continued*

```
  Dim Ver1, Ver2, Result
  Ver1 = GetVersionStringAsArray(Version1)
  Ver2 = GetVersionStringAsArray(Version2)
  If Ver1(0) < Ver2(0) Then
    Result = -1
  ElseIf Ver1(0) = Ver2(0) Then
    If Ver1(1) < Ver2(1) Then
      Result = -1
    ElseIf Ver1(1) = Ver2(1) Then
      Result = 0
    Else
      Result = 1
    End If
  Else
    Result = 1
  End If
  CompareVersions = Result
End Function
```

Listing 4: PowerShell Functions

```
# Bitwise left shift
function Lsh([UInt32] $n, [Byte] $bits) {
  $n * [Math]::Pow(2, $bits)
}

# Returns a version number "a.b.c.d" as a two-element numeric
# array. The first array element is the most significant 32 bits,
# and the second element is the least significant 32 bits.
function GetVersionStringAsArray([String] $version) {
  $parts = $version.Split(".")
  if ($parts.Count -lt 4) {
    for ($n = $parts.Count; $n -lt 4; $n++) {
      $parts += "0"
```

Listing 4: *continued*

```
    }
  }
  [UInt32] ((Lsh $parts[0] 16) + $parts[1])
  [UInt32] ((Lsh $parts[2] 16) + $parts[3])
}

# Compares two version numbers "a.b.c.d". If $version1 < $version2,
# returns -1. If $version1 = $version2, returns 0. If
# $version1 > $version2, returns 1.
function CompareVersions([String] $version1, [String] $version2) {
  $ver1 = GetVersionStringAsArray $version1
  $ver2 = GetVersionStringAsArray $version2
  if ($ver1[0] -lt $ver2[0]) {
    return -1
  }
  elseif ($ver1[0] -eq $ver2[0]) {
    if ($ver1[1] -lt $ver2[1]) {
      return -1
    }
    elseif ($ver1[1] -eq $ver2[1]) {
      return 0
    }
    else {
      return 1
    }
  }
  else {
    return 1
  }
}
```

Take care to note the syntax difference between VBScript and PowerShell when using these functions in your own code. In VBScript, function calls require parentheses with a comma between

Table 2: Functions Needed to Compare Versions

Function	Description
Lsh	Shifts a number left the specified number of bits.
GetVersionStringAsArray	Returns a version string *a.b.c.d* as two 32-bit values; uses the Lsh function.
CompareVersions	Compares two version strings. Returns -1 if the first version number is less than the second version, 0 if both version numbers are equal, or 1 if the first version number is greater than the second version; uses the GetVersionStringAsArray function.

parameters, whereas in PowerShell the parentheses and commas must be omitted. For example, in VBScript, you would write

```
Result = CompareVersions(Ver1, Ver2)
```

whereas in PowerShell, the equivalent code statement is

```
$Result = CompareVersions $Ver1 $Ver2
```

Download



Download the code

To see these functions in action, click the Download the Code icon. Versions.vbs and Versions.ps1 are standalone scripts that use these functions to let you compare file versions from the command line. The scripts contain some additional functions as well: Validate VersionString returns whether a specified version string is valid, and GetVersionArrayAsString is the inverse of GetVersionStringAsArray. I've also included a JScript version of the script, Versions.js, just in case JScript is your preferred language. ■

InstantDoc ID 142571

Product News for IT Pros

IceWarp Provides All-In-One Communications Infrastructure

Unless your Microsoft Exchange Server implementation is seriously ailing, moving to Exchange Server 2013 might be a low priority this year. Even if your business does need a messaging system upgrade, either to get off no-longer-supported software or to take advantage of new features, installing the new Exchange still might not be in the budget. Of course, you can consider Microsoft Office 365 if you want to keep it all in the Microsoft family and you're willing and able to take advantage of cloud services.

However, for companies that want to investigate options other than what Microsoft offers, it's always good to remember that other vendors do offer messaging servers that might just satisfy your needs. IceWarp has been in the market for over 10 years. The company's latest release, IceWarp Server 10.4.4, is compatible with Windows Server 2012 and Windows 8 and can be connected to Microsoft Outlook or can be used with IceWarp Desktop Client and IceWarp WebClient.

IceWarp Server provides all the expected business needs in a mail server—syncing email, calendar, contacts, and tasks—and it features built-in anti-spam and antivirus protection. Through add-ons, it can be configured to provide an integrated unified messaging environment, including IM, text messaging, and mobile device support. The IceWarp ecosystem is scalable to large enterprises—in fact, the IceWarp Server provides the back end for email service providers—but most customers come in the midrange, from 500 to 5,000 seats.

As far as why new customer are choosing IceWarp Server and where they're coming from, company president and co-founder Ladislav Goc said, "They're moving from Exchange because of the cost and because of the complexity of the maintenance. And second, they're actually

moving from the different kinds of open-source programs, free programs, or the smaller programs." IceWarp offers an all-in-one communications infrastructure, which can be deployed and maintained for less than the cost of Exchange, including the possibility of deploying on Linux servers, which should make this a good alternative to investigate for your messaging needs. For more information, see the IceWarp website.



Dell packetTrap RMM Upgrades Capabilities

The latest version of packetTrap's remote monitoring and management (RMM) platform is now available. With additional support capabilities, packetTrap introduces new features that offer the deepest network monitoring and management in the industry. This allows Managed Service Providers (MSPs) better control over clients' IT networks. Dell packetTrap RMM now fully supports Dell devices with performance monitoring, traffic analysis, and configuration backup. MSPs realize broader support for heterogeneous systems through a single solution that provides advanced visibility into network health, proactive analysis to minimize mean time to repair, and business savvy optimization across all network devices. MSPs interested in offering support for Windows 8 migrations can now do so with packetTrap RMM 6.7. Windows 8 enables providers to gain control and better support end users by proactively minimizing issues. It is also easier to manage and support an end user's mobile devices. For more information and a free fully featured trial of packetTrap RMM 6.7, visit the packetTrap website.



NetWrix Announces Activity Monitoring Software

NetWrix announced its new User Activity Video Reporter tool, which acts like a surveillance camera for critical servers and other IT systems by recording user activity for security, compliance, auditing, and troubleshooting. By capturing metadata during the recording process for reporting and playback, the VideoScape technology lets you fast-forward or link directly to specific tasks or actions. Tasks might include opening a window or starting a process, accessing or changing files,

web browsing, or working in management tools and applications. Complementing traditional configuration and change auditing solutions, NetWrix's new user activity monitoring software provides complete visibility of IT systems and applications that might not produce logs or enough information to investigate user behavior. Many critical systems require administrator or vendor accounts to be given extensive permissions that could allow them to circumvent any change and configuration logging. NetWrix User Activity Video Reporter can be used as a standalone product or as part of the NetWrix Change Reporter Suite. For more information, visit the Netwrix website.

Usoris Systems Brings Remote Printing and Enhanced RDP Support to Remote Utilities 5.4

Usoris Systems announced the release of Remote Utilities 5.4. The most prominent addition in version 5.4 is the remote printing feature. Users can now easily print a remote document on their local printer even if the originating software isn't installed on their system. Remote printing is also available in the Free Edition. Another new feature is the ability to connect in RDP mode while using the Internet ID firewall bypass technology. Previously, Remote Utilities could be used only as an RDP client for a direct IP connection, but now the program can work as a full-fledged transport for an RDP connection. The Viewer interface has been improved in version 5.4, too, and there is now a connection log in the Viewer that shows connection progress and helps with troubleshooting. For more information, see the Usoris Systems website.

Change Your Password from iPhone and iPad

BitsAbound announced the release of iCorpPass for iPhone, iPad, and iPod touch, allowing users to receive password expiry notifications as well as change passwords directly from the device. With iCorpPass, a user can directly log on to the corporate domain from his or her personal iPhone, iPad, or iPod touch device. The app automatically calculates the password expiry date and sets notifications on the device

to remind seven days, three days, and one day before the password expires. Users no longer need to call the Help desk to set a password, nor do they have to share their private passwords. They can change the password on their own, securely and from anywhere. BitsAbound's iCorpPass is an effective tool for organizations that use Active Directory (AD) as the central repository for user accounts and permissions, not only providing the freedom and ease that a modern user demands, but also helping IT departments with their password-reset and maintenance chores. Find more information at the BitsAbound website, and download the app from iTunes.





SecurEnvoy and PasswordBank Bring Tokenless Two-Factor Authentication to the Cloud

SecurEnvoy and PasswordBank have partnered on a solution that will let users access multiple cloud services at the same time. Through PasswordBank's single sign-on (SSO) platform, users will be able to access cloud solutions such as Google Apps, Office 365, and Salesforce.com, using SMS messages for two-factor authentication. This partnership delivers business-grade security, without requiring users to carry a physical token at all times. SecurEnvoy's Steve Watts said, "A major benefit of cloud technology is that it frees employees from their workstations, and gives them [mobile] access to the tools they need. Many companies implement two-factor authentication to ensure that they always know who is accessing their systems at any time. But forcing users to carry tokens around with them defeats the point. By combining the freedom of using SMS messages as the second factor, with the flexibility of the cloud, suddenly workers really do have the freedom they need." PasswordBank's Dennis Lee said, "By offering the tokenless solution from SecurEnvoy, we can meet the demands from our customers—and we can implement it with our current systems easily." For more information, visit the SecurEnvoy website and the PasswordBank website. ■

Goverlan Remote Control

Have you ever tried to assist a user over the phone with a Microsoft Word problem, only to learn that the user wasn't even using Word? Not being able to see a user's desktop, let alone control it, can really hinder an IT pro's ability to perform his or her job.

If this sounds familiar, you need a product like PJ Technologies' Goverlan Remote Control. It lets you quickly take control of a remote computer. You can either walk the user through the problem's resolution or take control of the computer and solve the problem yourself.



Eric B. Rux

is a contributing editor for *Windows IT Pro* and the manager of technical support services at a large university in eastern Washington.

Email

LinkedIn

Licensing

Goverlan's licensing is on a "per technician/computer" count and not a "per user" count. So, if you have five computer technicians who support 1,000 users, you need to purchase five licenses, not 1,000. If you have 20 technicians, but not all of them support users at the same time, you still need to purchase 20 licenses. Keep this in mind when comparing Goverlan with products that have a concurrent licensing scheme.

Each time you activate a license, your count is decremented by one. Activation can be done by Internet, email, or phone. Because the licenses are so tightly tied to the technicians' workstations, you need to remember to use the Activation Transfer Wizard (found under the Help menu) before rebuilding a technician's workstation.

Installation

Goverlan Remote Control is supported on Windows 2000 Professional and later (including Windows 8) and Windows 2000 Server through Windows Server 2008 R2. Installation is accomplished by a simple setup.exe routine. It packages a Windows Installer (.msi) file, so you can install Goverlan through Group Policy, Microsoft System Center Configuration Manager (SCCM), or another automated installation platform. Finally, you can install Goverlan using the following command:

```
GoverLANv7_Setup.exe /s /v/qn
```

Only one port (443) is used, so firewall configuration is kept to a minimum.

After the product is installed, the next step is to install the Goverlan Agent on each remote computer that you want to control. You can install it on all the computers in your network through the command line or your company's software distribution method (e.g., Group Policy, SCCM). The Goverlan Client Agent Installer directory, which is located where you installed Goverlan (C:\Program Files\Goverlan v7 by default), contains a prebuilt .msi file containing the agent. It also contains two files you can use to configure client-side settings: an .exe file if you're installing the agent from the command line and an .ini file if you're using Group Policy or SCCM to install the agent.

Alternatively, you can install the agent on an as-needed basis. Using the Goverlan Management Console, you simply right-click the client that you want to remotely control and choose Remote Control. If the agent isn't installed, you'll be prompted to install it at this time.

Features

I soon realized that Goverlan is much more than classic remote-control software. In addition to being able to take control of remote computers, Goverlan lets you perform advanced administrative tasks, such as displaying system information, adding software, managing Windows Automatic Updates, administering printers, opening a remote console, sending a popup message, opening a chat session, using Wake on LAN (WOL), and more. Two notable features are Scope Action and WMIX.

Scope Action. The Scope Action feature lets you control the computers on your network. For example, if you need all your client computers to update Group Policy, you can use a Scope Action to run a *gpupdate /force* command on each computer. Other examples include using a Scope Action to add or remove registry keys or file system objects (e.g., files, folders) from one or more computers.

The Scope Action feature is equally handy for reporting purposes. In just a few clicks, I was able to gather information about the computers on my network, such as each computer's name and system description, whether the computer is pingable and has Windows Firewall enabled, and who is currently logged on to that computer.

WMIX. Windows Management Instrumentation (WMI) has been around since Windows 2000. Unfortunately, it can be challenging to use if you're not versed in scripting. Goverlan's WMIX feature lets you use WMI within a GUI interface, without the need to learn a scripting language. After you define all the parameters of the WMI properties you want to query or edit, you click the Generate Script button to create a VBScript script that you can use.

Tight Active Directory Integration

I've seen quite a few administration applications in my years in IT. Many of them attempt to come up with their own management tool to group and manage computers and users. Goverlan doesn't do that—it uses your Active Directory (AD) organizational unit (OU) structure, which makes sense. You've (hopefully) organized your AD objects logically into a structure that works for your company. Goverlan does a great job of leveraging this structure, as Figure 1 shows. You can even add new computer, user, or group object right from this console instead of having to open up the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in.

After working with Goverlan for a while, I soon realized that this product is much more than classic remote-control software.

This integration doesn't stop at the management console. Configuring how the Goverlan agent behaves is controlled by a Group Policy Administrative Template (provided in both .adm and .admx files).

Support

Support is provided through a link on the Goverlan main page. Technical forums, white papers, user guides, training materials, and a knowledge base are all provided for free. Post-sales technical support requires that you have an active maintenance agreement. I found the

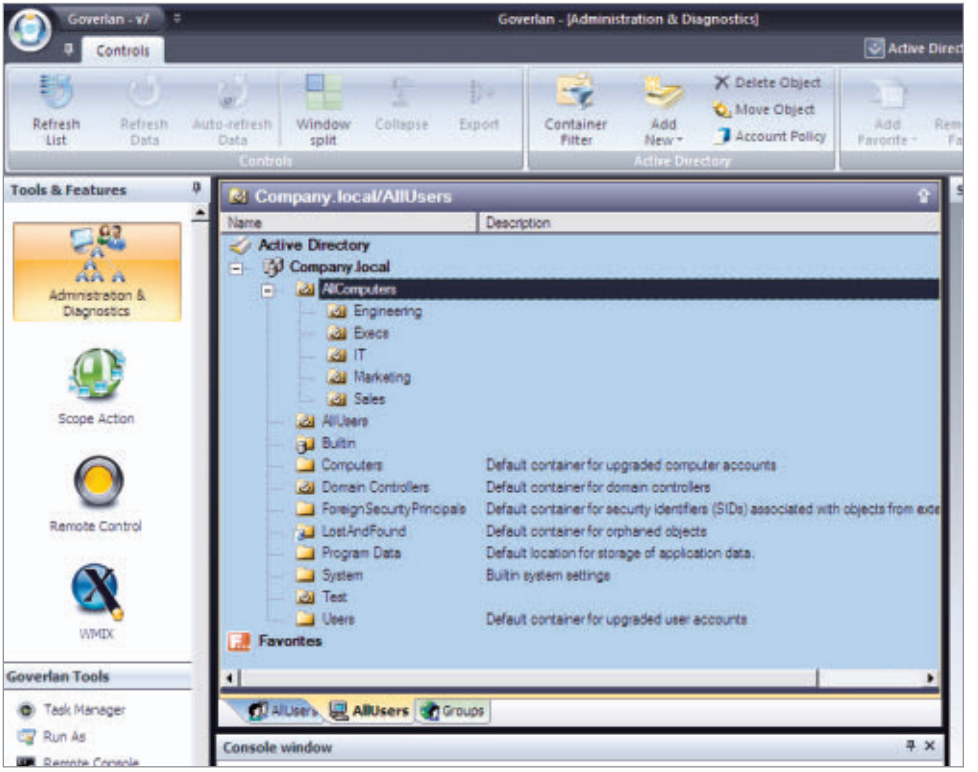


Figure 1
Goverlan's Integration Into the Existing AD OU Structure

support page to be logically laid out. The user guide was extremely helpful and was instrumental in setting up and understanding the product.

Remote-Control Capabilities and More

If you need simple remote-control software so that you can support your clients more effectively, then Goverlan is for you. If you need a complete client management solution that just happens to include remote-control capabilities, then Goverlan is definitely for you. The only "gotcha" I found with this product is the licensing model. If you have many technicians, the licensing might be an issue. However, if you only have a few people who need to use a tool like this, the licensing might not be a hurdle for you. ■

Goverlan Remote Control

PROS: Tight integration with AD OUs and Group Policy; easy to navigate the administrative console

CONS: Licensed per physical installation instead of a concurrent licensing model

RATING: ★★★★☆

PRICE: $299 per license or $119 per upgrade

RECOMMENDATION: If you have just a few technicians, the licensing model will probably work for you. If you need robust remote control and in-depth systems management, you owe it to yourself to give Goverlan a try.

CONTACT: PJ Technologies • 888-330-4188 or 786-268-3517

InstantDoc ID 144996

CloudPassage Halo

Managing Windows Server security can be a challenge once your server estate grows past a handful of devices. If you're not afraid of the command line, Windows Server 2012 provides effective management for larger server farms through Windows PowerShell. However, working exclusively with the command line can be a stiff learning curve for many administrators. In addition, getting quick results and interpreting data without a graphical interface isn't always ideal when you need to respond quickly to changing situations.

CloudPassage Halo is a Software as a Service (SaaS) offering that provides automated, scalable security protection for Windows and Linux servers that form a cloud infrastructure. Halo monitors security, alerts you about suspicious events, and provides strong firewall protection and multifactor authentication across your entire server farm.

Security as a Service

Halo runs a small, lightweight daemon (service) on each server that you want to monitor, which in turn connects to the Halo Grid. The grid runs in the cloud. It continuously collects data from each daemon and pushes policies to each monitored server. Events are recorded in a log in the management portal, which is called the Halo Portal. Halo can alert administrators immediately if a critical security event occurs.

To make security management as easy as possible, Halo uses server groups to assign policies. For example, you might place all web servers in a Halo server group and assign common firewall settings. GhostPorts provide a two-factor authentication mechanism that requires a user's Halo Portal password, plus a one-time password sent to the user's mobile phone. No special hardware is required, but Halo supports YubiKey hardware/software two-factor authentication in case it's needed.



Russell Smith

is an independent IT consultant specializing in systems management and security, and author of *Least Privilege Security for Windows 7, Vista and XP* (Packt).

Email

Twitter

Installing Halo

Installing and setting up Halo was simple. After I registered on CloudPassage's website, I logged on to the Halo Portal and downloaded the service daemon. I ran the installer on the server I wanted to protect and entered the domain registration code supplied on the download page.

Next, I logged on to the Halo Portal, where I saw the server listed on the Firewall Management tab, as shown in Figure 1. The first thing that struck me about the web management portal is the clean and simple lines, which make it easy to navigate without a steep learning curve.

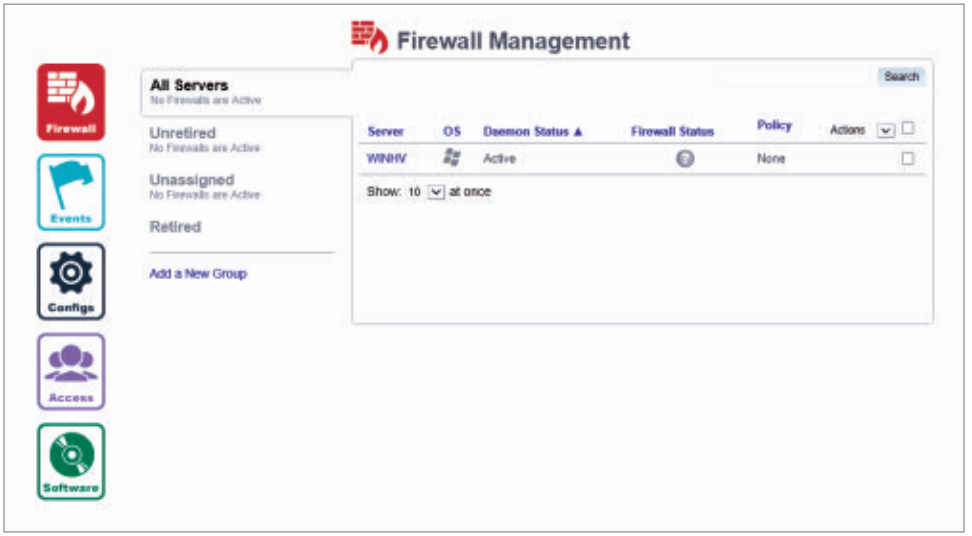


Figure 1
Firewall Management Tab of the Halo Portal

Server groups form the basis of all Halo configurations, so my first task was to create a new group named Standard in which to place my server. There's a link conveniently placed on the Halo Portal start screen to create a group. Selecting the *Add a New Group* link pops up a separate dialog box while graying out the background, ensuring that your attention is focused on the task at hand.

When you don't have any policies defined, creating a group is simply a matter of giving the group a name, optionally specifying a Server Tag, and clicking Save. You then move the server to the new group by selecting the server in the All Servers group, choosing Move Server(s) from

the Actions drop-down menu, and selecting the group. If you specify a Server Tag when you create a group, you don't need to manually move any new servers into that group. When you install the daemon on a new server, you just specify the Server Tag and the server will then be automatically added to the matching server group.

No matter what you do from the Halo Portal, it's impossible to lock yourself out of a server completely.

Configuring Halo Firewall Policies

After the group is populated with a server, you can create and apply some policies. Halo groups can have only one policy applied to them at a time. So, if you need to apply multiple firewall rules, they must all be listed in the same policy. It's important to understand that Halo is applying Windows Firewall rules and not its own firewall technology. As such, you'll be able to see Halo firewall rules in the standard Microsoft Management Console (MMC) Windows Firewall snap-in on servers managed by Halo. The rules applied by Halo are marked as CloudPassage rules to make them easy to identify.

When applying the first firewall policy, I was a little concerned that I might accidently lock myself out of the server by applying firewall rules through the Halo Portal. I noticed that apart from the standard core networking firewall rules that are present in Windows by default, all other default inactive inbound and outbound firewall rules were deleted. However, Halo adds default outbound rules for the daemon to ensure that access to the Halo Grid is always maintained.

As a simple test, I created an inbound firewall rule for secure POP3 from any IP address and blocked all other inbound access. There's a list of built-in network services to choose from, or you can define your own. Likewise, you can define your own IP address ranges and network interfaces. After I created the new policy, I edited the Standard group I created earlier and applied the new firewall policy. It took about a minute before the new policy became active on the server, which was noticeable as I was kicked out of my remote desktop session because I specified to block all incoming connections that didn't match the POP3 rule. To rectify this, I simply added another rule to the firewall policy to

allow incoming RDP traffic. Within a minute, I was able to get remote desktop access to my server again. The default heartbeat for the daemon is 60 seconds but can be increased up to 15 minutes.

Using GhostPorts

GhostPorts stops hackers from continuously scanning for open ports. It works by authorizing employees using two-factor authentication through the Halo Portal. It determines the user's source IP address and then modifies the server's firewall according to the GhostPorts rules that apply to the user, giving access to services and ports only from traffic identified to be from the user's IP address.

Halo Portal users need to be individually enabled to use GhostPorts. This is done by editing the user details in Site Administration under Settings. You can choose to use SMS codes or YubiKey. After the phone number of the user is entered, the user must confirm it by logging on to the Halo Portal again and entering a code sent to his or her phone. It should be noted that you can create standard user accounts in Halo Portal purely for the purposes of opening GhostPorts.

For this review, I tested SMS two-factor authentication. I enabled GhostPorts for my own administrative user account in the Halo Portal and changed the firewall rule I previously created to let inbound access for RDP port 3389 from any source IP address to this GhostPorts user (i.e., myself). This meant that in order to make a remote desktop connection to the server, I had to be logged on to the Halo Portal and authenticated using my Halo password and a code sent to my mobile phone by SMS.

After applying the rule, I first made sure that remote desktop access to my server was denied. I then re-authenticated on the Halo Portal. Once logged on, I clicked Open GhostPorts in the top right of the Halo Portal and confirmed that I wanted to send an authentication code to my mobile phone. After you enter the code into the Halo Portal, it displays the source IP addresses for the ports that will be opened according to the firewall policy and a note that you should wait for

a minute before trying to access the services. You get four hours of open access, or you can manually close ports by selecting the Close GhostPorts link in the top right of the Halo Portal.

Exploring Other Halo Features

Halo can log and alert you on what it calls special events. By default, all servers are covered by the global events policy, which contains a list of events such as *Server shutdown* and *Server moved to another group*. Some events are currently Linux only.

Alert profiles are easy to set up. You choose the kind of events you want to know about and the users to notify. Those users will then be alerted by email if the events occur.

Halo can run configuration checks to ensure servers meet certain conditions, such as running ACL checks on directories or confirming that a user has a password. However, all these checks apply to Linux only. At the time of this writing, CloudPassage was planning these features for Windows in early 2013. File integrity checking is also included in beta form.

Simple, Strong Security

One benefit of managing Windows Firewall using Halo is that no matter what you do from the Halo Portal, it's impossible to lock yourself out of a server completely—something that's quite possible if you're working with the MMC Windows Firewall snap-in directly. Although firewall policies should always be carefully planned, mistakes do happen. It's crucial not to be locked out of a remote server that can't be physically accessed for quick repair.

Halo is a good fit for small and large organizations alike. It's very easy to implement and provides advanced functionality in a form that can be easily deployed without a large outlay in infrastructure and hardware. Halo is a good option for any organization that needs to simplify but also strengthen cloud security. ■

InstantDoc ID 144906

CloudPassage Halo

PROS: Easy to set up; simplifies Windows Firewall management across multiple servers

CONS: Some features are Linux only; GhostPorts don't provide for computer authentication but can be used with standard IPsec security

RATING: ★★★★☆

PRICE: Firewall management free for up to five servers; subscriptions start from 3.5 cents per server-hour

RECOMMENDATION: Halo is a good option for any organization that needs to simplify but also strengthen cloud security. It's very easy to implement and provides advanced functionality in a form that can be easily deployed without a large outlay in infrastructure and hardware.

CONTACT: Cloud Passage • 415-886-3020

Windows 8 Tablets

Which one is right for you?



Paul Thurrott

is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows, a weekly editorial for *Windows IT Pro UPDATE*, and a daily Windows news and information newsletter called *WinInfo Daily UPDATE*.

Email

Twitter

Website

Windows 8 moves Microsoft's desktop OS firmly into the mobile OS arena for the first time. So it should come as no surprise that the devices on which Windows 8 runs have likewise expanded. Windows 8 is available on traditional portable and desktop PCs, of course, but also on a growing family of hybrid PCs, the most popular of which are tablets.

Although the range of Windows 8 tablets will no doubt eventually expand to encompass the same markets that competitors (e.g., the Apple iPad, Google Android-based tablets) currently occupy, this isn't the case today. Instead, Microsoft and its partners are focusing on productivity-first devices that combine work and play in a single form factor.

Left alone, at least for now, are so-called media tablets: devices that are aimed first at consumption activities such as digital music, video, and reading. This exception extends to the available hardware selection as well. You won't find any 7" tablets running Windows 8.

Architecture and Hardware Choices

Before you look at specific devices, some general choices will help you narrow the field. First and most obviously, Microsoft creates versions of Windows 8 for both traditional x86/x64 and ARM-based hardware.

The latter, called Windows RT, was ostensibly designed to facilitate super-thin and light iPad-like tablets with no fans and superior battery life. And on that note, Microsoft delivers. But Windows RT comes with one major disadvantage: It can't run most commonly available Windows desktop software (beyond the few utilities and handful of Microsoft Office 2013 applications that are included with the OS). This includes such things as browser add-ons such as Java and even Microsoft Silverlight, as well as hardware drivers for common devices.

It's worth noting that this limitation could be seen as a win, depending on your point of view. Windows RT systems likewise are more difficult than Windows 8 for malicious hackers to exploit. So if your needs are met by the currently lackluster selection of Metro-style apps that do run on Windows RT, then this OS could be a viable solution for you.

But thanks to some interesting innovations from the Intel camp, many Windows 8 tablets offer the form factor and mobility advantages of ARM-based devices but come with the hardware and software compatibility advantages of traditional x86/x64-based PCs. These systems run the new Intel Atom system on a chip (SoC) platform, code-named Clover Trail. Essentially a netbook-class platform, Clover Trail nonetheless runs performance rings around ARM-based devices, while offering similar battery life and the same fanless operation.

That said, Clover Trail–based devices are limited in a few of the same ways as ARM-based Windows devices. The key limitation is that they come with and support only 2GB of RAM, limiting their multitasking prowess. (By comparison, 4GB is the bare minimum on traditional PCs.)

As with other PCs, you can of course find Windows tablets based on Intel's mainstream x86/x64 Core chipset, code-named Ivy Bridge. These chips often bear names such asi3, i5, and i7. These tablets offer full compatibility with Windows desktop software and drivers—after all, they are essentially PCs—and offer the performance and RAM (4GB or more) required to run multiple applications simultaneously. However, these types of tablets are typically a bit thicker than ARM or Clover Trail devices. They come with fans and often run warmer and more loudly. And they get much less battery life—often just half that of their ARM and Clover Trail siblings.

While you weigh the tradeoffs of these three major Windows 8 tablet platforms, there are a few more hardware-related concerns to consider.

Multi-touch. All Windows 8–based tablets include pervasive multitouch capabilities. Don't discount the usefulness of this design even when used on traditional form factors such as Intel Ultrabooks or on

tablets that are docked or otherwise attached to a keyboard base. You will be surprised how quickly you get used to the multi-touch functionality—and how often you use it.

Pen/stylus. In keeping with their Tablet PC past, some Windows 8 keyboards include a stylus or pen. There are two types, and their capabilities vary widely. Capacitance pens work much like your finger but offer a slightly smaller tip, making it easier to tap small on-screen objects. However, they aren't very precise and are poor choices for handwriting. More sophisticated electromagnetic pens offer a smaller, more precise, and pressure-sensitive writing tip that is quite suitable for handwriting, as well as an eraser tip. Electromagnetic pens require more expensive screens than capacitive pens do, so they're typically found on higher-end devices.

Sensors. Windows 8 supports a wide range of new hardware sensors, although some will be more common than others. Typical sensors include GPS (for location), accelerometer (for acceleration), gyroscope (for device positioning in 3D space, usually for games), compass, and light (for adaptive screen brightness). If you want to use your Windows 8 tablet as a giant GPS in the car, for example, you might want to look for one with a GPS (and possibly broadband cellular capabilities, although you might be able to share your phone's connection instead).

OK, let's talk devices. In the world of Windows 8 tablets, there are basically three: a pure tablet, detachable device, and convertible device.

Pure Tablet: Microsoft Surface

Microsoft and its partners don't yet offer any real media tablets; the smallest Windows 8 tablets are about as close as we can get these days. I think of these tablets, which offer screens smaller than 11", as "pure" tablets: Their small size means that they will be used as touch-capable tablets most frequently. This is true even though they typically offer clip-on keyboards or keyboard bases. Of course, they can be used with Bluetooth-based wireless keyboards.

The pure tablet market is most obviously represented by the Microsoft Surface lineup, which currently consists of two models, both of which offer 10.6" screens housed in stunning, industrial-grade magnesium alloy casing. Both work with excellent Type Cover and Touch Cover accessories, which provide surprisingly good typing experiences, and a handful of other add-ons. But beyond these similarities, the two models are quite different under the hood.

Surface with Windows RT (which Figure 1 shows) shipped in late October 2012. As its name suggests, it runs on the ARM platform, so it can't utilize traditional Windows desktop software, browser add-ons, or drivers. It features 2GB of RAM and 32GB or 64GB of solid state disk (SSD) storage. The device costs $500 to $730, depending on the storage configuration and cover type. (The base version comes sans cover.) The device features a single USB 2.0 port and micro-SD storage expansion. And it delivers more than 8 hours of battery life in real-world use.



Figure 1
Surface with Windows RT

Surface with Windows 8 Pro began shipping in early February 2013. It features a 1.7GHz Intel Core i5-3427U microprocessor, 4GB of RAM, and 64GB or 128GB of SSD storage. It costs $900 to $1,000, depending on configuration. The device features a single USB 3.0 port (with a second built into the power adapter) and micro-SD storage expansion. But unlike the Surface RT, which uses a 1366 × 768 display, the Surface Pro has a full-HD screen with 1920 × 1080 resolution. The Surface Pro is also heavier (2 pounds versus 1.5 pounds) and a bit thicker.

Because the Surface Pro uses a standard Core i5 part, there are concerns about fans and heat. But early previews of the device suggest that its unique active cooling system, in which heat is ushered silently out of the device through vents, seems to work. I will need to test this

system extensively before I feel comfortable declaring it a success. I do know that real-world battery life is about 5 hours, however.

Based on my own testing, I can't really recommend Surface with Windows RT, given that comparable Clover Trail–based machines offer better compatibility and performance with similar form factors and battery life. But the Surface form factor obviously has a future, and the coming months will determine whether Surface Pro, or some future Surface device, marks the breakthrough.

Detachable: Samsung ATIV Smart PC

Although the Surface devices are unique because of their reliance on Type and Touch Covers, a broader range of tablets are shipping with detachable hardware keyboards. These devices, which I call detachables, will likely make up the mainstream portable-computing market in just a few short years. You might think of them as Ultrabooks with detachable screens.

A detachable keyboard—or a keyboard dock, as these items are often called—offers some important advantages over the Surface's lighter Touch and Type Covers. These pros include additional USB and other ports and, in some models, a second battery for even more endurance. Detachables come in a wide range of sizes, but the most common right now is 11.6", which doesn't seem like a big leap from the Surface's 10.6" unit but is in reality a huge difference. As a case in point, the Samsung ATIV Smart PC range includes two models: the Clover Trail–based Smart PC 500T, which I've used extensively, and the Ivy Bridge–based Smart PC 700T.



Figure 2
Samsung Smart PC 500T

The 500T, which Figure 2 shows, features a 1.8GHz Intel Atom Z2760 processor, 2GB of RAM, 64GB of SSD storage, a

1366 × 768 display, and a single USB 2.0 port. This device beats out the Surface RT in virtually every category that matters, while offering a real hardware keyboard dock with two more USB 2.0 ports (though no additional battery). The 500T gets more than 9 hours of real-world battery life.

The 700T, like the Surface Pro, uses an Intel Core i5-3317U processor, 4GB of RAM, 128GB of SSD storage, and a full HD 1920 × 1080 display, albeit one that's easier on the eyes thanks to the larger form factor. It, too, has a single USB 3.0 port, but you get two additional USB 2.0 ports on the keyboard dock. The battery life is rated at 5 to 8 hours, depending on usage.

Choosing between the two—or similar competitors—comes down to a compromise between performance and price. The 500T outperforms Surface RT handily, but it's basically a glorified and expensive netbook tablet. The 700T, meanwhile, is the real deal but is quite expensive at about $1,200.

Convertible: Lenovo IdeaPad Yoga

As odd as Windows 8 is with its dual user experiences, it shouldn't come as any surprise that PC makers are trying out some unusual designs. Sure, there are traditional convertible tablets similar to what we saw with the initial generation of Tablet PCs a decade ago. Such devices can transform between a laptop-like form factor and a tablet (albeit a heavy one; you can't physically detach the keyboard from the screen).

And then there are the gymnasts—my name for the machines that can really bend, twist, swivel, and contort. And not just into two form factors; these devices can convert into three or four positions.

The poster child for this crazy new kind of device is the Lenovo IdeaPad Yoga, which ships in three basic models. Each is a rather sedate-looking device. But looks—and first impressions—can be deceiving. Each Yoga model can be used in four forms:

- A typical Ultrabook form factor
- A tablet form factor

- Tent mode (in which you bend the screen over the back and position it like an inverted V for content consumption)
- Stand mode (in which you put the screen on the bottom for passive content consumption, such as movie watching)

Lenovo makes an 11.6" Yoga 11 with Windows RT, but I recommend choosing between the 11.6" Yoga S and the 13" Yoga 13 (which Figure 3 shows). Both devices run Windows 8. Both ship with a range of true Core processors, 4GB to 8GB of RAM, and 128GB or 256GB of SSD storage. The Yoga S features a 1366 × 768 screen, although I prefer the great 1600 × 900 display on the Yoga 13 that I tested. The Yoga S gets about 5 to 6 hours of battery life, compared with a bit over 6 hours for the Yoga 13.



Figure 3
Lenovo IdeaPad Yoga

If you're a bit gun-shy on the tablet front, the Yoga and rival convertibles represent a good value and can be used solely in a traditional, Ultrabook-like form factor, until you're more comfortable experimenting on the multi-touch wild side.

Key Take-Aways

So which of these devices best suits you? Surface and other pure tablets are a good choice for those who want to use the device as a tablet first, with occasional productivity. Detachables offer the best of both worlds, with ideal form factors for both consumption and productivity. And convertibles are a great choice for those who value productivity over consumption but want options for both. Take your pick! ■

InstantDoc ID 145121

Insights from the Industry

OWA 2013: Good Enough to Replace Outlook?

With the release of Microsoft Exchange Server 2013, it's perhaps time again to turn some attention to Outlook Web App (OWA). As usual, the Exchange team devoted some useful development time to providing enhancements to OWA 2013. The new ability for offline mail access has probably received the most attention, but other interesting changes include the dramatically simplified UI and the ability to integrate apps with OWA (which also applies to the Outlook 2013 desktop client). The question naturally arises about whether OWA is good enough to allow companies to abandon Outlook on the desktop in favor of OWA. Let's examine the new features a little closer to see what benefits they bring.

Offline access. You can use OWA to read and respond to email even when you have no network connection, which could be great. However, this feature is possible only with the very latest browser—Microsoft Internet Explorer (IE) 10, Apple Safari 5, and Google Chrome 18—and enabling offline access is sure to require a good deal of end-user training to avoid security problems. Whether this feature is truly a boon remains to be seen, but in the short term, I suspect many organizations would rather avoid using it.

Simplified UI. The simplified UI seems largely to be a winner, although there are always users who have valid disagreements with changes made to the features they interact with the most. The look and feel might be cleaner, but can you easily find the functions you use every day? Microsoft believes you'll be able to. Perhaps we should expect an adjustment period before writing off the UI changes as bad. However, if



B. K. Winstead

is a senior associate editor for *Windows IT Pro, SQL Server Pro*, and *SharePoint Pro*, specializing in messaging, mobility, and unified communications.

Email

Twitter

Blog

access to a feature simply isn't in the UI, such as Public Folders in OWA 2013, that's going to be a problem for anyone who needs such access.

One reason for the UI change is to present a consistent view of the OWA environment across different browsers and on different devices, such as desktops, laptops, and tablets, including those with touch capabilities. Although I haven't been able to test this experience personally, the demonstrations I've seen (granted, given by Microsoft people) certainly make switching from one device to another look quite seamless. The fact that this sort of design effort was even made seems to be a recognition of the work habits of a modern workforce. People work everywhere and they want the same connected experience on whichever device they choose *at the moment*. OWA 2013 should be able to provide that experience.

Ability to integrate apps. For me, the new model for integrating apps with Outlook and OWA seems one of the most exciting new features in this round, but how well it's received largely depends on whether developers get on board and build third-party add-ons. At launch, you'll have the Bing Maps app and a few others. The Bing Maps app can provide a graphic map and directions for meeting invitations, which can certainly be handy. At the Microsoft Exchange Conference (MEC) 2012, Messageware introduced one of the first third-party apps for Outlook, Messageware TakeNote, a tool that lets you add notes to messages or senders. If you're into coding yourself, you can learn about developing Outlook apps in the Microsoft article "Mail apps for Outlook."

These are all great features in their own ways, but I'm not sure if they really offer enough in themselves to sound the death knell for the Outlook fat client. Another factor that often enters the debate at this point is cost. Can your business save money by using only OWA and avoiding the whole desktop upgrade? In the past, this point swung in OWA's favor, but with the Office 2013 suite available in a subscription model, the answer is less clear. Maybe you can upgrade without the high upfront costs.

Then the question comes back to whether Outlook 2013 provides anything compelling that OWA 2013 doesn't. Building on the Outlook Social Connector add-in introduced for Outlook 2010, one of the biggest changes for Outlook 2013 is the People Hub, which is the new standard view for contacts. You can link multiple versions of the same person, including information from LinkedIn and other social networks, so everything appears on a single contact card. But you can also do that in OWA 2013.

The other UI change for Outlook 2013 is the Weather bar on the calendar, which gives you a three-day snapshot of your local weather forecast (or some other region if for some reason you've configured it that way). This feature is a pretty neat idea, but not a dealmaker. The rest of Outlook 2013's enhancements are mostly around performance improvements and back-end stuff, all of which is of no consequence if you decide to use only OWA.

As Microsoft continues to develop in tandem the cloud and on-premises versions of products, you have to wonder what the future is for the desktop version of Outlook. Sparked by reading a blog by Kerio's Andrew Staples, "Long live email, but desktop email clients are dead (or at least dying)," I posed the question "Is Outlook dead/dying?" on Twitter. Twitter user @getgander replied, "Maybe 'stagnant' is the best word? I think as generations change, Outlook may fade, but right now, it has an incumbent advantage." And Exchange MVP Devin Ganger (@devinganger) said, "Outlook will die when admin assistants use something else to manage delegate calendars. Not today!"

You can probably build a case for using either Outlook or OWA with Exchange 2013. Of course, the whole debate is meaningless if you're not planning to upgrade to Exchange 2013 in the first place. But if you are, it might well be worth considering what experience will best suit the needs of your users and your business when you're up and running in the new Exchange environment.

—B. K. Winstead

InstantDoc ID 144921

PowerShell Plus Available for Free



Blair Greenwood

is editorial assistant for *Windows IT Pro, SQL Server Pro*, and *Dev Pro*. She holds a bachelor's degree in technical journalism from Colorado State University. She's worked with Java, C, and Visual Basic programming languages.

Email

Twitter

Idera has released a new version of its integrated development environment (IDE), PowerShell Plus 4.6. In addition, the company is showing its support for the PowerShell community by making the IDE available for free. The release also coincides with Microsoft's delivery of Windows 8 and Windows Server 2012, which features the full integration of Windows PowerShell 3.0.

Several PowerShell experts have stressed the exigency for PowerShell expertise in IT environments. In "Getting Started with PowerShell," PowerShell MVP Don Jones stated that PowerShell expertise is a more reliable indicator of skillfulness than any Microsoft examination. "If you think certifications were a key to you getting and maintaining your job, then make no mistake: PowerShell is even more crucial. Ignore it at your peril," said Jones.

Sharing a similar sentiment, PowerShell MVP Thomas Lee said, "With the new capabilities in PowerShell 3.0 and its tight integration with Microsoft's next generation server and desktop products, it is the future of both Windows administration and the development of manageable enterprise applications." In addition, Lee said that the IDE's increased accessibility now empowers users to easily and quickly learn PowerShell while improving the accuracy and speed of their scripting.

Winning gold in *Windows IT Pro's* Editors' Best awards for best scripting tool in 2012, Idera's PowerShell Plus provides an interactive console that features an advanced script editor, debugger, and learning center that lets IT professionals quickly learn and master PowerShell. The new version of PowerShell Plus has been certified on Windows 8 and includes revised and enhanced script libraries for SQL Server and SharePoint 2010. In addition, the product's System Explorer now features SQL Server and SharePoint 2010 plug-ins that help manage SQL Server instances and SharePoint 2010 farms. Visit the PowerShell Plus product page to learn more. ■

InstantDoc ID 144990

The New Windows Ecosystem

Take a moment to appreciate it!



Jason Bovberg

Email

Twitter

Website

The tech landscape is pretty exciting these days, with Microsoft's introduction of a few new OSs (Windows Server 2012, Windows 8, and Windows RT) as well as the company's all-new tablet computer, which comes in two forms: the iPad-competing Surface RT and the powerful Surface Pro. Surface is the first touch-enabled tablet straight from Microsoft. And it's a flawed beauty.

The Surface—and, by extension, Microsoft's entire new Windows 8 ecosystem—is big news, especially for those of us interested in powerful productivity devices. I've resisted the iPad since its debut, simply because it always seemed like an expensive toy to me. I just couldn't justify the price for a consumption device that didn't offer me a compelling experience that I couldn't get on my existing devices and systems. I guess when I get right down to it, I wanted to be able to work on it, to get stuff done. And in my line of work, that means I wanted to be able to write on it.



So when it was revealed that Microsoft would be producing a tablet computer that would bring to the market a full "laptop computing" experience, my interest was piqued. Reading the specs, I saw that the Surface would feature a cover that doubled as a physical keyboard—and I knew that would make all the difference.

For my overall computing experience, I've always yearned for a sense of convergence. I've quietly hoped that Microsoft would come up with a media experience that would marry with my existing Windows work and home experiences. It just made sense that something like that would come to pass.



An exciting development toward that sense of Windows convergence was the introduction of Windows Phone. In fact, Windows Phone's unique tile-based interface was a key origin of Windows 8's new interface. So far, market acceptance of Windows Phone has been meager, at best. A frustrating development! Windows Phone is a beautiful option for those who aren't bowled over by the same ol' iOS interface of the iPhone and the copycat interface of the Android phone. But Microsoft took forever to come up with a great phone—way too long. It finally has that great phone, but in many ways, the market is already set in stone, and newcomers have very little footing. Will Windows Phone suffer the same fate as the Zune music device?

Microsoft isn't betting on it. Rather than let its critically acclaimed "new look" fade into the background in a competitive market, the company is not only doubling down on it but tripling (maybe quadrupling) down. The new tiles-based interface is present on the new Xbox 360 interface, on the new Windows Phone 8 smartphones, on the Surface tablets, and on all new Windows 8 PCs and laptops. In short, Microsoft is all in on this interface.

And that's the convergence I've been seeking.

From the point of view of this Windows user, who also happens to be a writer, the Surface is an exciting piece of hardware, despite its first-generation problems (comparatively low battery life, no 3G/4G connectivity, storage concerns). There's no denying that Surface is an entirely new beast that should appeal to a lot of power users. I look forward to taking my Surface on the road and doing productive, keyboard-necessary work wherever the mood strikes—and using the same device for media consumption when that mood strikes.

It's taken too long, but Microsoft is finally getting it right. I'm glad to be excited again about the technology company I've been using for years. ■

Send us your funny screenshots, oddball product news, and hilarious end-user stories. If we use your submission, you'll receive a *Windows IT Pro* Rubik's Cube.

Submit

Directory of Services

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

- Cloud & Virtualization UPDATE
- *Dev Pro* UPDATE
- Exchange & Outlook UPDATE
- Security UPDATE
- *SharePoint Pro* UPDATE
- *SQL Server Pro* UPDATE
- *Windows IT Pro* UPDATE
- WinInfo Daily UPDATE

RELATED PRODUCTS

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the web. Includes FREE access to eBooks and archived eLearning events plus a subscription to either *Windows IT Pro* or *SQL Server Pro*.
www.windowsitpro.com/go/vipsub

SQL Server Pro

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

Dev Pro

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

Advertiser Directory

1&1 Internet 1

Entensys 18

NWN 22, 23

Windows IT Pro 2

Vendor Directory

5nine Software 67

Amazon 79

Apple 14, 61, 76, 79, 106

BitsAbound 95, 96

Centrify 26

CloudPassage 101, 103, 105

Concur Technologies 27

Dell 64

Emulex 64

F5 Networks 66

Google 10, 14, 76 , 106

Google Apps 27

HP 60, 64

IceWarp 93, 94

Identropy 27, 28

Idera 116

Intel 64, 107, 109, 110, 111

Lenovo 111, 112

Messageware 114

Mozilla 76

nAppliance Networks 66

NEC 67

NetWrix 94, 95

Nicira 73

Novell 79

Okta 25, 27

OneLogin 25, 27

packetTrap 94

PasswordBank Technologies 96

Ping Identity 26

PJ Technologies 97, 100

Radiant Logic 26

Salesforce.com 27

Samsung 61, 110

SecurEnvoy 96

sFlow 67

Symplified 25, 27

Usoris Systems 95

Windows IT Pro